INFORME AUDITORÍA

A fin de mantener actualizadas las políticas de protección de datos y revisar las medidas y procedimientos aplicados, así como la correcta adecuación de las mismas a los sistemas de tratamiento e información que tratan los datos personales bajo la responsabilidad de la entidad, periódicamente se realizarán auditorías para detectar todas aquellas deficiencias que puedan existir en los protocolos en materia de protección de datos, procediendo a la actualización de los mismos cuando sea necesario.

CONVERSIA

ÍNDICE

1. INTRODUCCIÓN

Una auditoría es un proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría. Estos criterios son el conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia de la auditoría. Las evidencias de la auditoría son aquellos registros, declaraciones de hechos o cualquier otra información que es pertinente y verificable.

La realización de la auditoría supone una evidencia que demuestra la responsabilidad proactiva (*Accountability*) del artículo 24 apartado 1, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, por el cual se establece que: "Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*"*

Asimismo, la realización de la auditoría supone la concreción de lo establecido en el artículo 32 apartado 1 letra d), del citado reglamento, por el cual se establece que: *"*Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros, un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento."

2. OBJETO, ALCANCE DE LA AUDITORÍA E IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

2.1. OBJETO Y ALCANCE

El presente informe se elabora y entrega como resultado del encargo de trabajo a PROFESSIONAL GROUP CONVERSIA SLU, que se produjo tras la aprobación de la correspondiente propuesta presentada a EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL el año 2022, para la realización de una auditoría de los sistemas de información e instalaciones de tratamiento de datos y la emisión de un dictamen de auditoría, relativo a los procedimientos e instrucciones vigentes en materia de seguridad de datos.

Se pretende emitir un informe independiente y objetivo, de tal forma que el Responsable del tratamiento, tome las medidas oportunas para subsanar las no conformidades identificadas, si las hubiera, y atender las recomendaciones realizadas por el auditor.

2.2. OBJETIVO DE LA AUDITORÍA

El objetivo final de la auditoría y del presente informe de auditoría es mantener actualizadas las políticas de protección de datos y revisar las medidas y procedimientos aplicadas, así como la correcta adecuación de las mismas a los sistemas de tratamiento e información que tratan los datos personales bajo la responsabilidad de la entidad, así como detectar todas aquellas no conformidades que puedan existir en los protocolos en materia de protección de datos, procediendo a la actualización de los mismos cuando sea necesario. Todo ello, teniendo en cuenta la metodología de gestión de la mejora continua basada en cuatro etapas: Plan (Planificar), Do (Hacer), Check (Verificar), Act (Actuar).

2.3. NORMATIVA APLICABLE

El proceso de auditoría así como los controles auditados se han fundamentado en la legislación vigente en materia de protección de datos de carácter personal y normativa complementaria, utilizando como normativa de referencia y contraste los siguientes documentos:

a) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

b) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

c) Leyes y reglamentos vigentes en materia de seguridad de datos.

d) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

e) Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

f) Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

g) Guía de Seguridad de las TIC CCN-STIC 802 – ENS. Guía de auditoría.

h) Recomendaciones, informes y guías vigentes de la Agencia Española de Protección de Datos.

i) Informes jurídicos de la Agencia Española de Protección de Datos.

j) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

k) Real Decreto 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la Ley 15/1999

de Protección de Datos de Carácter Personal.

l) Ley orgánica 34/2002 de 11 de Julio, Servicios de la Sociedad de la Información y de Comercio Electrónico.

m) Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

n) Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

o) Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

p) Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n° 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión.

q) Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

r) Circular de la Fiscalía 1/2016, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.

2.4. ESTÁNDARES UTILIZADOS

En los últimos años se ha incrementado la atención sobre los controles internos, tanto para los auditores, los gerentes, o para las entidades reguladoras en general. Como resultado de un continuo y trabajoso esfuerzo, se han desarrollado varios documentos para definir, valorar, reportar y mejorar el control interno, y ser utilizados como marco de referencia en las organizaciones. Para el desarrollo de la presente auditoría, se han tomado en consideración los siguientes estándares:

a) UNE-ISO/IEC 27001 – Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).

b) UNE-ISO/IEC 27002 – Tecnología de la información, Técnicas de seguridad, Código de buenas prácticas para los controles de seguridad de la información.

c) UNE-ISO 19011:2011 – Directrices para la auditoría de los sistemas de gestión.

d) UNE 19601:2017, Sistemas de Gestión Compliance Penal.

e) UNE-ISO 19600:2015 de Sistemas de Gestión de Compliance.

f) Informe COSO - (Committee of Sponsoring Organizations), de la Comisión de Estudios de Controles Internos.

g) SAC - (Systems Auditability and Control), de la Fundación de Investigación del Instituto de Auditores Internos.

h) SAS 55 y SAS 78 - Consideraciones de la estructura de Controles Internos en los Informes de los Estados Financieros, del Instituto Americano de Contadores Públicos (CPA).

i) COBIT (Control Objectives for Information and related Technology), de la Fundación de Auditoría y Control de Sistemas de Información.

Cada uno de ellos ha sido definido para una audiencia en particular: el "COSO" fue diseñado para la Gerencia; el "SAC" para los auditores internos; los SAS 55 y SAS 78 para los auditores externos, y finalmente el "COBIT" enfocado principalmente a los auditores de sistemas de información.

2.5. FECHA DE REALIZACIÓN DE LA AUDITORÍA

Se realiza la auditoría de los sistemas de información e instalaciones de tratamiento de datos de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL para la anualidad de 2022 y la entrega del presente informe a 7 de marzo de 2022.

2.6. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

RAZÓN SOCIAL: EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL

NIF: G66546581

DIRECCIÓN FISCAL: FLORIDABLANCA 146 3 1 08011, BARCELONA

3. FASES DEL TRABAJO DE AUDITORÍA

El trabajo de auditoría se ha desarrollado cumpliendo los plazos establecidos.

Las fases en que se ha dividido el desarrollo de las distintas actuaciones han sido las siguientes:

1. Inicio de la auditoría
   1.1 Identificación de los interlocutores

2. Preparación de las actividades de auditoría
   2.1. Recogida de información
   2.2. Preparación del plan de auditoría
   2.3. Preparación de los documentos de trabajo

3. Realización de las actividades de auditoría
   3.1. Recopilación y verificación de la información
   3.2. Revisión de la documentación
   3.3. Comunicación durante la auditoría
   3.4. Estudio y análisis de la información
   3.5. Preparación de las conclusiones de la auditoría

4. Preparación del informe de auditoría

5. Aclaraciones

6. Entrega y distribución del informe

4. REALIZACIÓN DE LA AUDITORÍA

La auditoría y su respectivo informe se han realizado tras la revisión de los sistemas de información y de la documentación de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL situada en FLORIDABLANCA 146 3 1 08011, BARCELONA.

Tanto el trabajo de auditoría como la elaboración del informe de auditoría han sido desarrollados por un equipo de profesionales con las competencias necesarias para garantizar la adecuada realización de la auditoría y el dictamen correspondiente, trabajando simultáneamente los aspectos técnicos y organizativos de la seguridad, la privacidad, así como los legales.

Para la ejecución de este encargo de auditoría, se han llevado a cabo las siguientes acciones:

- Realización de la auditoría mediante entrevistas.
- Revisión de documentos.
- Análisis y revisión de las medidas, controles y procedimientos de seguridad de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL.
- Elaboración del informe de auditoría.

Calendario de entrevistas

Para el desarrollo del trabajo de auditoría y elaboración del informe se han realizado las siguientes entrevistas:

LUGAR	AÑO	NOMBRE Y APELLIDOS	CARGO
BARCELONA	2022	DAVID PERE MARTINEZ ORO	Representante Legal

Lista de distribución

Este informe de auditoría debe ser entregado a las siguientes personas pertenecientes a la organización del Responsable del Tratamiento:

NOMBRE Y APELLIDOS	CARGO Y DEPARTAMENTO
DAVID PERE MARTINEZ ORO	Representante Legal
DAVID PERE MARTINEZ	Responsable de Privacidad
DAVID PERE MARTINEZ	Responsable de Seguridad
DAVID PERE MARTINEZ	Responsable de Sistemas

5. DOCUMENTACIÓN REVISADA

Para el desarrollo del trabajo de auditoría y elaboración del informe se ha analizado la siguiente documentación:

TÍTULO DEL DOCUMENTO	ORIGINAL O COPIA	BREVE REFERENCIA DEL CONTENIDO
RECURSOS PROTEGIDOS	COPIA	Descripción de los distintos recursos protegidos utilizados en la entidad y activos que intervienen en la misma, tipología de activo así como su ubicación y su responsable.
ESTRUCTURA Y ROLES DE PRIVACIDAD	COPIA	Documento donde se definen los diferentes roles dentro de la entidad, así como las obligaciones legales y funciones de cada una de las figuras que se nombran.
NORMATIVA DE SEGURIDAD	COPIA	Procedimientos y protocolos para reducir el riesgo respecto la seguridad y privacidad de los datos de carácter personal que posee la entidad.
PROCEDIMIENTO DE GESTIÓN DE LOS DERECHOS DE LOS INTERESADOS	COPIA	Modelo y procedimiento para el ejercicio de los derechos por parte de los interesados contemplados en la normativa aplicable y vigente en materia de protección de datos.
CLÁUSULAS LEGALES DE INFORMACIÓN	COPIA	Cláusulas legales en cumplimiento con el deber de información y transparencia.
COMPROMISO DE CONFIDENCIALIDAD	COPIA	Documento de confidencialidad para los empleados de la entidad.
COMUNICADO INTERNO	COPIA	Documento utilizado para comunicar a los empleados de la entidad, las funciones y obligaciones que deben cumplir en el desarrollo de sus funciones.
CONTRATOS DE PRESTACIÓN DE SERVICIOS	COPIA	Contratos de prestación de servicios que debe firmar la entidad con Terceros que les presten algún tipo de servicio que pueda conllevar un tratamiento de datos de carácter personal responsabilidad de la entidad.
ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIÓN	COPIA	Registro de prestadores de servicios que puedan acceder a los sistemas de información a través de accesos remotos.

PROCEDIMIENTO DE COMUNICACIÓN ANTE UNA VIOLACIÓN DE SEGURIDAD DE LOS DATOS	COPIA	Procedimiento para establecer un canal de comunicación con el Delegado de Protección de Datos o en su defecto el Responsable de Privacidad, con la finalidad de gestionar las violaciones de seguridad de los datos.
IDENTIFICACIÓN Y AUTENTICACIÓN	COPIA	Relación de los usuarios existentes que tratan datos de carácter personal en cada uno de los distintos equipos informáticos.
REGISTRO DE ACTIVIDADES DE TRATAMIENTO	COPIA	Documento donde se ha diseñado un registro de las operaciones de tratamiento de datos personales.
CONTROL DE ACCESO FÍSICO	COPIA	Documento donde se detalla la relación de aquellas personas, externas a la entidad, que acceden periódicamente a las instalaciones para prestar su servicio, pudiendo acceder accidentalmente, a datos de carácter personal.
RELACIÓN DE ENCARGADOS DEL TRATAMIENTO	COPIA	Relación de los prestadores de servicio autorizados a acceder a los datos de carácter personal para la prestación del servicio.
RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE UBICACIÓN DE LOS SISTEMAS INFORMÁTICOS	COPIA	Relación de los dispositivos portátiles de la entidad.
PROCEDIMIENTO DE COPIAS DE SEGURIDAD Y RECUPERACIÓN	COPIA	Procedimiento utilizado para la realización de copias de seguridad y recuperación de datos.
INVENTARIO DE APLICACIONES INFORMÁTICAS	COPIA	Documento donde se recoge la relación de aplicaciones existentes para el tratamiento de datos en cada uno de los equipos informáticos de la entidad.
PLAN DE CAPACITACIÓN PARA LA APLICACIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS	COPIA	Procedimiento para implantar un plan de formación.

PROCEDIMIENTO DE GENERACIÓN DE PROCESOS DE TRATAMIENTO DE DATOS	COPIA	Modelo gráfico del proceso a seguir para la iniciación de nuevas operaciones de tratamiento
POLITICA DE OPERACIONES DE TRATAMIENTO NO AUTOMATIZADAS	COPIA	Documento donde se establece el criterio de archivo, de los dispositivos de almacenamiento, la copia y reproducción, el traslado y el acceso a la documentación. Habilitación de un formulario para las autorizaciones al personal al que se le deba autorizar acceso a datos de categoría especial
PROCEDIMIENTO DE GESTIÓN DE SOPORTES	COPIA	Documento donde se define el procedimiento para la identificación, inventario y custodia de todos los soportes, tanto físicos como en formato electrónico que contengan datos de carácter personal.

PROFESSIONAL GROUP CONVERSIA SLU, con plena libertad, ha aceptado el encargo de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL para realizar una auditoría de controles de protección de datos y el informe sobre la misma, al objeto de verificar si los sistemas de información e instalaciones de tratamiento de datos responsabilidad de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL cumplen con lo establecido en la normativa vigente en materia de Protección de Datos, los procedimientos en el mismo obrantes, así como las instrucciones vigentes dictadas por la Agencia Española de Protección de Datos en materia de seguridad de datos.

PROFESSIONAL GROUP CONVERSIA SLU garantiza que dicha auditoría ha sido realizada conforme a las condiciones, duración, alcance y régimen económico establecidos y bajo los criterios de independencia, imparcialidad y objetividad, y sin otras limitaciones que las impuestas por la ley, las normas éticas y deontológicas.

PROFESSIONAL GROUP CONVERSIA SLU ha cumplido con su objetivo de realizar la auditoría de medidas de seguridad y el informe correspondiente sobre la misma con el máximo celo y diligencia. Guardará el secreto profesional por tiempo indefinido sobre todos los datos, hechos y observaciones de los que tenga conocimiento así como sobre las valoraciones que realice por razón de cualquiera de las modalidades de su actuación profesional. Ha acometido este encargo ateniéndose a las exigencias técnicas, deontológicas y éticas adecuadas a la tutela de dicho asunto, habiéndose apoyado para ello en sus colaboradores y otros compañeros, quienes han actuado bajo su responsabilidad, guardando el mismo nivel de secreto y con las mismas exigencias técnicas, deontológicas y éticas.

La realización de la auditoría se ha realizado debidamente, sin limitaciones ni restricciones que pudieran entorpecer la labor del equipo auditor.

6. MEDIDAS VERIFICADAS

La realización de la auditoría en EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL, así como el presente informe de auditoría se han llevado a cabo respecto a las siguientes medidas, procedimientos y controles en materia de seguridad de datos:

Controles

Para toda la tipología de tratamientos:

- Control de acceso de los usuarios a los datos y recursos que precisan para el desarrollo de sus funciones
- Controles periódicos para verificar el cumplimiento de lo que dispone el Sistema de Gestión de la Privacidad
- Control de la existencia y cumplimiento de las medidas definidas en el Sistema de Gestión de la Privacidad por el Responsable de seguridad/privacidad
- Dictamen del informe de auditoría para comprobar la existencia de controles en cumplimiento de la normativa en protección de datos

Procedimientos

Para toda la tipología de tratamientos:

- Procedimiento de notificación, gestión y respuesta ante las incidencias y/o brechas de seguridad
- Procedimiento de realización de las copias de respaldo
- Procedimiento de recuperación de los datos
- Procedimiento de identificación para el acceso de los usuarios al sistema de información
- Procedimiento de autentificación para el acceso de los usuarios al sistema de información
- Procedimiento de asignación, distribución y almacenamiento de contraseñas

Medidas

Para toda la tipología de tratamientos:

- Acceso a datos a través de las redes de comunicación
- Régimen de trabajo fuera de los locales de ubicación del fichero
- Ficheros temporales
- Documento de Seguridad/Documentación de Medidas y Procedimientos de seguridad y privacidad de los datos
- Funciones y obligaciones del personal
- Gestión de soportes
- Realización de una auditoría bienal
- Control de acceso físico

7. OPERACIONES DE TRATAMIENTO

A continuación, se describen brevemente las operaciones de tratamiento realizadas por EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL así como los colectivos y tipologías de datos objeto de tratamiento:

Nombre del tratamiento:	Control de acceso y presencialidad con sistema de fichaje	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Empleados		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Firma		Meramente identificativo	

Nombre del tratamiento:	Gestión del cumplimiento normativo asociación	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Clientes, Empleados, Usuarios, Proveedores, Asociados y miembros, Junta directiva, Asistentes		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Teléfono		Meramente identificativo	
NIF		Meramente identificativo	
Dirección Postal		Meramente identificativo	
Dirección electrónica		Meramente identificativo	
Firma		Meramente identificativo	
Datos profesionales de empleo		Meramente identificativo	
Datos económicos de seguros		Meramente identificativo	

Nombre del tratamiento:	Gestión asociados y/o miembros	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Asociados y miembros		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Teléfono		Meramente identificativo	

NIF	Meramente identificativo
Dirección Postal	Meramente identificativo
Dirección electrónica	Meramente identificativo
Firma	Meramente identificativo
Datos de salud	Categoría especial

Nombre del tratamiento:	Gestión de nóminas y contratos	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Empleados		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Teléfono		Meramente identificativo	
NIF		Meramente identificativo	
Dirección Postal		Meramente identificativo	
Nº Seguridad Social		Meramente identificativo	
Características Personales		Meramente identificativo	
Datos académicos		Meramente identificativo	
Datos profesionales de empleo		Meramente identificativo	
Datos económicos de seguros		Meramente identificativo	

Nombre del tratamiento:	Usuarios web	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Usuarios web		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Dirección electrónica		Meramente identificativo	
Dirección IP		Meramente identificativo	

Nombre del tratamiento:	Gestión de los miembros de la Junta Directiva	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Junta directiva		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	

Nombre	Meramente identificativo
Teléfono	Meramente identificativo
NIF	Meramente identificativo
Dirección Postal	Meramente identificativo
Características Personales	Meramente identificativo
Dirección electrónica	Meramente identificativo
Firma	Meramente identificativo
Datos profesionales de empleo	Meramente identificativo
Datos económicos de seguros	Meramente identificativo

Nombre del tratamiento:	Gestión económica y administrativa asociación	**Sistema de tratamiento:**	Informatizado
Colectivo/s de afectados:	Clientes, Usuarios, Proveedores, Asociados y miembros, Asistentes		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Teléfono		Meramente identificativo	
NIF		Meramente identificativo	
Dirección Postal		Meramente identificativo	
Datos económicos de seguros		Meramente identificativo	

Nombre del tratamiento:	Gestión de RRHH	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Empleados, Recursos humanos		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Teléfono		Meramente identificativo	
NIF		Meramente identificativo	
Dirección Postal		Meramente identificativo	
Características Personales		Meramente identificativo	
Dirección electrónica		Meramente identificativo	
Firma		Meramente identificativo	
Datos académicos		Meramente identificativo	
Datos profesionales de empleo		Meramente identificativo	
Imagen y/o voz		Meramente identificativo	

Nombre del tratamiento:	Gestión de las formaciones y/o cursos	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Asistentes		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Teléfono		Meramente identificativo	
NIF		Meramente identificativo	
Dirección Postal		Meramente identificativo	
Características Personales		Meramente identificativo	
Dirección electrónica		Meramente identificativo	
Datos académicos		Meramente identificativo	
Datos profesionales de empleo		Meramente identificativo	

Nombre del tratamiento:	Gestión de los usuarios	**Sistema de tratamiento:**	Mixto
Colectivo/s de afectados:	Usuarios		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Teléfono		Meramente identificativo	
Dirección electrónica		Meramente identificativo	
Datos de salud		Categoría especial	

Nombre del tratamiento:	Tratamiento de imágenes asociación	**Sistema de tratamiento:**	Informatizado
Colectivo/s de afectados:	Empleados		
DATOS OBJETO DE TRATAMIENTO			
Datos		**Tipología**	
Nombre		Meramente identificativo	
Imagen y/o voz		Meramente identificativo	

Nombre del tratamiento:	Participación en la investigación de Mercado	**Sistema de tratamiento:**	Mixto

Colectivo/s de afectados:	
DATOS OBJETO DE TRATAMIENTO	
Datos	**Tipología**
Nombre	Meramente identificativo
NIF	Meramente identificativo

8. CRITERIOS NORMATIVOS: IDENTIFICACIÓN DE LAS NO CONFORMIDADES Y PROPUESTA DE MEDIDAS CORRECTORAS

8.1. PRINCIPIOS RELATIVOS AL TRATAMIENTO

DEFINICIÓN

“Artículo 5. Principios relativos al tratamiento

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).”

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto a los principios de licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad establecidas en el Reglamento General de Protección de Datos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha constatado que los datos personales objeto de tratamiento son los estrictamente necesarios y, además, se mantienen actualizados.

Se ha constatado que los datos personales se almacenan o custodian más tiempo del informado en el momento de la recogida de los datos.

Se verifica que existe un procedimiento para la supresión de los datos una vez ha expirado el plazo previsto. Dicho procedimiento no es adecuado.

Se ha verificado que los datos recabados son adecuados, pertinentes, no excesivos y proporcionales a la finalidad prevista.

Se ha constatado que no existen finalidades incompatibles, y que se han tenido en cuenta la compatibilidad de las mismas en caso de existir algún cambio en la propia finalidad de la operación de tratamiento.

Se ha verificado que se han previsto medidas de seguridad para evitar que los sistemas de información pierdan la disponibilidad.Se ha constatado que disponen medidas técnicas y organizativas para garantizar la integridad de los datos personales tratados, conservados y/o transmitidos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

Se ha verificado que se han establecido medidas para garantizar la confidencialidad de los datos personales.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá revisar el procedimiento para la supresión de los datos una vez expirado el plazo de conservación ya que no se considera adecuado para la finalidad prevista.

Se deberán almacenar o custodiar los datos el plazo informado en el momento de la recogida de los datos.

RECOMENDACIONES DEL AUDITOR

No proceden.

8.2. RESPONSABILIDAD PROACTIVA (ACCOUNTABILITY)

DEFINICIÓN

“Artículo 5. Principios relativos al tratamiento

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 24. Responsabilidad del responsable del tratamiento

1**.** Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 25. Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.”

Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo. EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL deberá adoptar medidas preventivas dirigidas a reducir los riesgos de incumplimiento y, además, deberá estar en condiciones de demostrar que ha implantado esas medidas y que las mismas son las adecuadas para lograr la finalidad perseguida.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto al principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha procedido a estudiar y determinar la necesidad de llevar a cabo una Evaluación de Impacto.

Se ha procedido a analizar el riesgo de las operaciones de tratamiento efectuadas.

Se ha procedido a constatar que se han realizado auditorías de los sistemas de información en los dos últimos años. Tras el examen realizado a la documentación aportada por EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL, se constata que existen no conformidades en la auditoría realizada el año anterior.

Se ha constatado que la empresa no dispone de alguna certificación en materia de seguridad de la información, protección de datos y/o cumplimiento legal.

Se ha verificado que se dispone de un procedimiento de formación en materia de protección de datos.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se recomienda implantar a EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL todas las medidas correctoras propuestas en las auditorías anteriores.

RECOMENDACIONES DEL AUDITOR

Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. La certificación será voluntaria y estará disponible a través de un proceso transparente.

8.3. LICITUD DEL TRATAMIENTO

DEFINICIÓN

“Artículo 6. Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar

si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7. Condiciones para el consentimiento

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8. Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.”

“Artículo 9. Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de

datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona

sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.”

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la licitud de los tratamientos según el Reglamento General de Protección de Datos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha constatado que cuando el tratamiento se basa en el interés legítimo del responsable del tratamiento, se procede a ponderar este interés legítimo respecto a los derechos y libertades de los interesados.

Se ha constatado que cuando el tratamiento se basa en el consentimiento del interesado, el responsable del tratamiento no es capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

Se ha procedido a verificar que cuando el tratamiento se basa en el consentimiento del interesado, se facilita la posibilidad de retirar el consentimiento prestado.

Se ha constatado que se ha considerado una base legítima para los tratamientos realizados.

Se ha constatado que EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL trata datos personales de categorías especiales y que concurre alguna de las circunstancias del artículo 9 apartado2 por el cual se habilita el tratamiento de categorías especiales de datos personales.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Deberá disponer de documentos que acrediten la obtención del consentimiento de los interesados para el tratamiento de sus datos.

RECOMENDACIONES DEL AUDITOR

No proceden.

8.4. DEBER DE INFORMACIÓN Y TRANSPARENCIA

DEFINICIÓN

“Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Artículo 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o

histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria."

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto a los principios de información y transparencia establecidos en el Reglamento General de Protección de Datos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha verificado que en el momento de la recogida de los datos se proporciona información respecto a los tratamientos que se llevan a cabo.

Se ha procedido a constatar que en el momento que se obtienen los datos personales se informa de la identidad y los datos de contacto del responsable.

Se ha verificado que en el momento que se obtienen los datos personales se informa de los fines del tratamiento.

Se ha verificado que en el momento que se obtienen los datos personales se informa de la base jurídica del tratamiento.

Se ha verificado que en el momento que se obtienen los datos personales se informa del plazo de conservación o de los criterios utilizados para determinar el plazo.

Se ha verificado que en el momento que se obtienen los datos personales se informa de la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y a su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.

Se ha verificado que en el momento que se obtienen los datos personales se informa del derecho a presentar una reclamación ante una Autoridad de Control.

Se ha verificado que EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL realiza cesiones y que en el momento que se obtienen los datos personales se proporciona información relativa a los destinatarios o las categorías de destinatarios de los datos personales.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos (artículo 6, apartado 1, letra f)), se deberá facilitar información relativa a los intereses legítimos de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL o de un tercero.

Cuando el tratamiento esté basado en el consentimiento o consentimiento explícito del interesado (artículo 6, apartado 1, letra a) o el artículo 9, apartado 2, letra a)), se deberá facilitar información relativa a la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

Cuando EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL utilice los datos personales para un fin que no sea aquel para el que se recogieron deberá proporcionar al interesado, información sobre ese otro fin y cualquier información adicional pertinente.

EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL podrá dar cumplimiento al deber de información facilitando al afectado la información básica e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. La información básica deberá contener, al menos:

- La identidad del responsable del tratamiento y de su representante, en su caso.

- La finalidad del tratamiento.

- La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

8.5. DERECHOS DE LOS INTERESADOS

DEFINICIÓN

“Artículo 15. Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia, mencionado en el apartado 3, no afectará negativamente a los derechos y libertades de otros.

Artículo 16. Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17. Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18. Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20. Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Artículo 21. Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.”

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto al derecho de acceso, derecho de rectificación, derecho de supresión (“el derecho al olvido”), derecho a la limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición y derecho a no ser objeto de decisiones individuales automatizadas.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha constatado que se ha establecido un procedimiento para atender el ejercicio del derecho de acceso por parte de los interesados y este es adecuado y acorde con los requisitos establecidos en la normativa aplicable y vigente en materia de protección de datos. Pero no se aplica de forma correcta.

Se ha constatado que se ha establecido un procedimiento para atender el ejercicio del derecho de rectificación por parte de los interesados y este es adecuado y acorde con los requisitos establecidos en la normativa aplicable y vigente en materia de protección de datos. Pero no se aplica de forma correcta.

Se ha constatado que se ha establecido un procedimiento para atender el ejercicio del derecho de supresión (“el derecho al olvido”) por parte de los interesados y este es adecuado y acorde con los requisitos establecidos en la normativa aplicable y vigente en materia de protección de datos. Pero no se aplica de forma correcta.

Se ha constatado que se ha establecido un procedimiento para atender el ejercicio del derecho a la limitación del tratamiento por parte de los interesados y este es adecuado y acorde con los requisitos establecidos en la normativa aplicable y vigente en materia de protección de datos. Pero no se aplica de forma correcta.

Se ha constatado que se ha establecido un procedimiento para atender el ejercicio del derecho a la portabilidad de los datos por parte de los interesados y este es adecuado y acorde con los requisitos establecidos en la normativa aplicable y vigente en materia de protección de datos. Pero no se aplica de forma correcta.

Se ha constatado que se ha establecido un procedimiento para atender el ejercicio del derecho de oposición por parte de los interesados y este es adecuado y acorde con los requisitos establecidos en la normativa aplicable y vigente en materia de protección de datos. Pero se ha comprobado que el procedimiento no se aplica de forma correcta.

Se ha constatado que no se ha recibido ninguna solicitud de ejercicio de derechos.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá aplicar de manera efectiva el procedimiento para atender el ejercicio del derecho de acceso.

Se deberá aplicar de manera efectiva el procedimiento para atender el ejercicio del derecho de rectificación.

Se deberá aplicar de manera efectiva el procedimiento para atender el ejercicio del derecho de supresión.

Se deberá aplicar de manera efectiva el procedimiento para atender el ejercicio del derecho de limitación.

Se deberá aplicar de manera efectiva el procedimiento para atender el ejercicio del derecho de portabilidad.

Se deberá aplicar de manera efectiva el procedimiento para atender el ejercicio del derecho de oposición.

RECOMENDACIONES DEL AUDITOR

EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

Cuando EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

8.6. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

DEFINICIÓN

“Artículo 30. Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destina-tarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el Encargado del Tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.”

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto a la obligación de llevar y mantener un registro de las actividades de tratamiento por escrito, así como si dicho registro contiene la información establecida en el Reglamento General de Protección de Datos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha verificado que se lleva a cabo un registro de las actividades de tratamiento que contiene la información indicada en el artículo 30 apartado 1 del Reglamento General de Protección de Datos y que se mantiene actualizado.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL deberá poner el registro a disposición de la autoridad de control que lo solicite.

8.7. FUNCIONES Y OBLIGACIONES DEL PERSONAL

8.7.1. DOCUMENTACIÓN PARA LA ORGANIZACIÓN INTERNA

DEFINICIÓN

El personal que tenga acceso a datos de carácter personal para el desempeño de las funciones propias de su puesto de trabajo, tiene la obligación de colaborar con el Responsable del Tratamiento para velar por el cumplimiento de la legislación vigente sobre Protección de Datos de Carácter Personal, asimismo debe respetar los procedimientos definidos para gestionar la seguridad de la información.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto a la información proporcionada al personal de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL, acerca de las medidas de seguridad, controles y procedimientos que debería cumplir en materia de protección de datos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha constatado que EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL dispone de personal.

Se comprueba la existencia de un modelo de circular interna que contiene las obligaciones y deberes a tener en cuenta por el personal en el desarrollo de sus funciones, así como las consecuencias de su incumplimiento conforme a lo dispuesto en la normativa de protección de datos. Dicha circular se difunde al personal de la entidad.

Se comprueba la existencia de un compromiso de confidencialidad por el cual, el personal adquiere el compromiso de velar por la seguridad y el buen uso de los datos personales y donde se establece la información necesaria para tratar los datos de los mismos. Dicho compromiso se ha difundido y firmado por el personal de la entidad.

Se verifica que se han comunicado al personal las políticas y procedimientos de seguridad que debe adoptar durante el desarrollo de sus funciones.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

Se recomienda a EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL que cuando se incorpore nuevo personal se le entregue la circular interna y se recabe firmado el correspondiente compromiso de confidencialidad para que pueda garantizar que ha informado a su personal de las medidas que deberá adoptar para dar cumplimiento a la normativa aplicable y vigente en materia de protección de datos.

8.7.2. ROLES EN MATERIA DE PRIVACIDAD

DEFINICIÓN

De acuerdo con todo aquello previsto en la normativa vigente y aplicable en protección de datos, EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL, a fin de organizar y gestionar adecuadamente sus políticas de protección de datos, ha estructurado su organización en base a distintos roles, a los cuales se les atribuyen distintas funciones en materia de privacidad.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto a la asignación de los roles de privacidad.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha verificado que se ha nombrado a un responsable de privacidad. Dicho nombramiento ha sido debidamente firmado.

Se ha verificado que se ha nombrado a un responsable de seguridad. Dicho nombramiento ha sido debidamente firmado.

Se ha verificado que se ha nombrado a un responsable de sistemas. Dicho nombramiento ha sido debidamente firmado.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

No proceden.

8.8. PRESTACIÓN DE SERVICIOS

DEFINICIÓN

“Artículo 28. Encargado del Tratamiento.

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

> a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
>
> b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
>
> c) tomará todas las medidas necesarias de conformidad con el artículo 32;
>
> d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;
>
> e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;
>
> f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
>
> g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;
>
> h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.
>
> En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.”

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto a la elección de los encargados del tratamiento, la subcontratación a otros encargados y las estipulaciones mínimas del contrato u acto jurídico que regirá el tratamiento por parte del encargado, así como el nivel de cumplimiento respecto a las empresas sin acceso a datos de carácter personal para la prestación del servicio pero que pudieran acceder a datos de manera accidental o involuntaria.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se verifica que existen terceras personas o empresas que prestan servicios a EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL.

Tras la revisión de los correspondientes contratos de prestación de servicios se observa que éstos están debidamente firmados.

Se ha verificado que cuando se contrata a un prestador de servicios para el tratamiento de datos personales no se selecciona de manera adecuada.

Se ha verificado que existe una relación de los prestadores de servicios con acceso a datos y que no está actualizada.

SALVEDADES

No existen.

PROPUESTAS DE MEDIDAS CORRECTORAS

Se deberá elegir a un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme a los requisitos del Reglamento General de Protección de Datos y garantice la protección de los derechos del interesado.

Se recomienda establecer una relación actualizada de los prestadores de servicios con acceso a datos.

RECOMENDACIONES DEL AUDITOR

Se recomienda a EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL que en el caso de tener nuevos prestadores de servicios que accedan a datos de carácter personal formalicen un contrato de prestación de servicios según lo establecido en el artículo 28 del Reglamento General de Protección de Datos.

Se recomienda a EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL que en el caso de tener nuevos prestadores de servicios que puedan acceder a datos de carácter personal de forma accidental o involuntaria formalicen un acuerdo de confidencialidad.

8.9. VIDEOVIGILANCIA

DEFINICIÓN

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

“Artículo 22. Tratamientos con fines de videovigilancia

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica."

"Artículo 89. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley."

DATOS, HECHOS Y OBSERVACIONES

Se ha constatado que EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL no dispone de un sistema de videovigilancia, por lo que no procede realizar una verificación del cumplimiento.

VERIFICACIÓN DE SU CUMPLIMIENTO

No procede.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

No proceden.

8.10. EVALUACIÓN DE IMPACTO

DEFINICIÓN

“Artículo 35. Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las

repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.”

DATOS, HECHOS Y OBSERVACIONES

Se ha constatado que EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL no tiene la obligatoriedad y/o necesidad de llevar a cabo una Evaluación de Impacto de determinadas operaciones de tratamiento, por lo que no procede realizar una verificación del cumplimiento.

VERIFICACIÓN DE SU CUMPLIMIENTO

No proceden.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

No proceden.

8.11. DELEGADO DE PROTECCIÓN DE DATOS

DEFINICIÓN

“Artículo 37. Designación del delegado de protección de datos

1. El responsable y el Encargado del Tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el Encargado del Tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el Encargado del Tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del Encargado del Tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el Encargado del Tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38. Posición del delegado de protección de datos

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.”

DATOS, HECHOS Y OBSERVACIONES

Se ha detectado que EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL no dispone de Delegado de Protección de Datos, dado que no lo ha designado de forma voluntaria y no le es requerido por la normativa aplicable y vigente en materia de protección de datos, por lo que no procede realizar una verificación del cumplimiento.

VERIFICACIÓN DE SU CUMPLIMIENTO

No procede.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

No proceden.

8.12. TRANSFERENCIAS DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

DEFINICIÓN

“Artículo 44. Principio general de las transferencias

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el Encargado del Tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45. Transferencias basadas en una decisión de adecuación

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6. La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46.Transferencias mediante garantías adecuadas

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el Encargado del Tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el Encargado del Tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el Encargado del Tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47. Normas corporativas vinculantes

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del Encargado del Tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las

normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48. Transferencias o comunicaciones no autorizadas por el Derecho de la Unión

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o Encargado del Tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49. Excepciones para situaciones específicas

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el Encargado del Tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.”

DATOS, HECHOS Y OBSERVACIONES

Se ha constatado que EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL no realiza transferencias internacionales de datos personales, por lo que no procede realizar una verificación del cumplimiento.

VERIFICACIÓN DE SU CUMPLIMIENTO

No procede.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

No proceden.

9. CRITERIOS DE SEGURIDAD: IDENTIFICACIÓN DE LAS NO CONFORMIDADES Y PROPUESTA DE MEDIDAS CORRECTORAS

9.1. SEGURIDAD FÍSICA

La seguridad física es una parte fundamental para la protección de la información. Por tanto, para diseñar e implantar un plan de seguridad adecuado se deberá tener en cuenta la protección física.

En este apartado, se analiza la existencia de un conjunto de políticas y procedimientos que EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL ha considerado adecuadas para minimizar los riesgos a un nivel aceptable. Entre ellos, destacamos:

- Protección frente amenazas ambientales.
- Puntos de acceso.
- Ubicación y protección en los equipos.
- Protección en el cableado.
- Control de acceso físico.

9.1.1. PROTECCIÓN FRENTE AMENAZAS AMBIENTALES

DEFINICIÓN

La protección frente amenazas externas y ambientales es aquella que hace referencia a las amenazas que se ve expuesta la entidad ante eventos causados por la naturaleza y las acciones realizadas por la intervención humana, ya sea de forma intencionada o accidental.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la existencia de la política de protección frente amenazas externas y ambientales y, si dicha política, se ha hecho efectiva.

VERIFICACIÓN DE SU CUMPLIMIENTO

No se dispone de una política respecto a la protección de los locales propios de la organización frente a las amenazas ambientales.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá diseñar una política frente amenazas ambientales para evitar riesgos producidos por desastres naturales, accidentes o bien amenazas provocadas por la acción humana como por ejemplo revueltas sociales.

RECOMENDACIONES DEL AUDITOR

Contratación de servicios de asesoramiento especializado para evitar daños en la entidad, concretamente en los datos de carácter personal, provocados por inundaciones, fuego, explosiones o, bien, aquellos provocados la acción humana como revueltas sociales o sabotajes.

9.1.2. PUNTOS DE ACCESO

DEFINICIÓN

Los puntos de acceso son aquellas áreas dentro de la entidad donde puede acceder personal no autorizado como pueden ser las áreas de carga y descarga o bien las áreas de recepción.

El control de dichos puntos permite maximizar la seguridad respecto a los accesos no autorizados y, así, evitar riesgos directos a la información tratada por la entidad.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la existencia de un procedimiento en referencia a los puntos de acceso expuestos a personal no autorizado como áreas de recepción, áreas de carga y descarga, entre otras.

Además, se comprueba la existencia de un procedimiento de revisión de recepción de material que pudiera derivar amenazas potenciales como explosivos o productos químicos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de un procedimiento respecto a los puntos de acceso de la entidad para evitar la exposición de datos de carácter personal a personal no autorizadopero no se mantiene actualizado.

La entidad no aplica de forma activa dicho procedimiento.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el procedimiento respecto a los puntos de acceso de la entidad siempre que exista algún cambio en los mismos.

Se deberá aplicar de forma activa el presente procedimiento para evitar el acceso a datos de carácter personal a personas no autorizadas e, incluso, contemplar en el procedimiento, la verificación de recepción de material para evitar amenazas potenciales como explosivos, productos químicos o cualquier otro material potencialmente peligroso como pueden ser dispositivos de almacenamiento infectados con programas maliciosos.

RECOMENDACIONES DEL AUDITOR

- Contemplar restricciones en los accesos en dichas áreas.
- Inspección de material entrante en los puntos de acceso (al público) para evitar amenazas potenciales, ya sea de tipo explosivos, productos químicos, etc. o, bien, dispositivos (memorias USB, *CD-Roms*, etc) maliciosos.

9.1.3. UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS

DEFINICIÓN

La colocación de las estaciones de trabajo o cualquier dispositivo cuya finalidad sea la del tratamiento de datos de carácter personal deberá situarse y protegerse de manera que minimice los riesgos ante las amenazas ambientales, así como, evitar los accesos a personal no autorizado.

DATOS, HECHOS Y OBSERVACIONES

Verificación de la existencia de un plan para evitar el riesgo de pérdida, daño, robo o cualquier otro compromiso de los activos de información y su posible interrupción en las operaciones de tratamiento de datos de carácter personal.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de un plan para evitar el riesgo de pérdida, daño, robo o cualquier otra amenaza en los activos de información y en los tratamientos de datos de carácter personalpero no se mantiene actualizado.

No se aplica de forma activa el presente plan.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el plan respecto a la ubicación de los equipos siempre que exista algún cambio físico o bien exista alguna necesidad.

Se deberá dar a conocer a todo el personal implicado el presente plan y aplicarlo de forma activa para evitar pérdidas, daños, robos o cualquier amenaza a los activos de información y, a su vez, a la afectación de las operaciones de tratamiento de datos de carácter personal.

RECOMENDACIONES DEL AUDITOR

Minimizar los accesos innecesarios en las áreas de trabajo.

- En los tratamientos de datos de carácter especial evitar exponer dicha información a personas no autorizadas.
- Establecer mecanismos contra accesos no autorizados en los sistemas de almacenamiento.

9.1.4. SUMINISTROS EN LOS EQUIPOS

DEFINICIÓN

Los sistemas de tratamiento de información deberán contar con alternativas para estar protegidos ante fallos eléctricos u otras alteraciones causadas por fallos en las instalaciones de suministros.

Todo suministro redundante para prevenir la indisponibilidad de los sistemas de tratamiento deberían contar principalmente con inspecciones regulares para asegurar su correcto funcionamiento y disponer de alarmas ante fallos de funcionamiento.

DATOS, HECHOS Y OBSERVACIONES

Se verifica la existencia de una política para los suministros alternativos para prevenir la indisponibilidad de los sistemas de tratamiento.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de una política respecto a las instalaciones de suministro para evitar fallos de alimentación e interrupción de las comunicaciones. Dicha política no se mantiene actualizada.

EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL no aplica de forma activa la presente política.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizada la política de instalaciones de suministros para evitar fallos de alimentación e interrupción de las comunicaciones.

Se deberá aplicar de forma activa la presente política de instalaciones de suministros.

RECOMENDACIONES DEL AUDITOR

Se puede maximizar la disponibilidad eléctrica y de comunicaciones mediante redundancia de los servicios. En referencia al suministro eléctrico se podría considerar la instalación de sistemas de alimentación ininterrumpida (SAI) y, para la disponibilidad de comunicación, la contratación de un proveedor de servicios adicional.

9.1.5. PROTECCIÓN EN EL CABLEADO

DEFINICIÓN

El cableado eléctrico y el de telecomunicación no quedan exentos de amenazas de interceptación de información, interferencias en las comunicaciones o bien daños físicos que afecten a la disponibilidad o integridad de la información.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la existencia de medidas de seguridad en el cableado, tanto eléctrico como el de telecomunicaciones para evitar riesgos de interferencias, interceptaciones de información en las comunicaciones o bien daños físicos en los mismos.

VERIFICACIÓN DE SU CUMPLIMIENTO

No se dispone de una política respecto a la protección del cableado para evitar riesgos de interferencias, interceptaciones o daños físicos en los mismos.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá diseñar una política, y a su vez aplicarla de forma activa, respecto a la protección del cableado para evitar riesgos de interferencias, interceptaciones o daños físicos en los mismos.

RECOMENDACIONES DEL AUDITOR

Se aconseja que la instalación del cableado eléctrico y el de telecomunicación no queden expuestos a la vista para evitar manipulaciones no autorizadas.

Además, es conveniente poder separar las dos tipologías de cableado para evitar interferencias en los mismos.

9.1.6. GESTIÓN DE CAMBIOS

DEFINICIÓN

Los cambios generados dentro de la entidad deben ser registrados para tener un control actualizado y que afecte a la seguridad de la información. Dichos cambios pueden ser a nivel organizativo, operaciones de tratamiento y procesos asociados, instalaciones de tratamiento de información y los propios sistemas que traten datos personales.

DATOS, HECHOS Y OBSERVACIONES

Se verifica si la entidad tiene controlados los cambios que se producen y que afectan, o pueden afectar, a la seguridad de la información. Además, para ello, se debe registrar y comunicar a las personas involucradas de dichos cambios, ya sean de tipo procesos del negocio o cambios en las instalaciones de tratamiento de información.

VERIFICACIÓN DE SU CUMPLIMIENTO

No se dispone de un procedimiento para la gestión de cambios dentro de la entidad y, por tanto, no dispone de un control actualizado del mismo ni de los procedimientos que le puedan afectar cualquier cambio.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá diseñar un procedimiento de control de gestión de cambios, ya sean los que afecten a procesos clave de la entidad o bien aquellos que afecten a los sistemas o instalaciones y que puedan afectar a la seguridad de la información.

RECOMENDACIONES DEL AUDITOR

Un control inadecuado de los cambios que existen en la entidad puede provocar un aumento de los riesgos en materia de seguridad de la información. Los cambios incontrolados en el entorno operativo pueden impactar en la fiabilidad de las aplicaciones o bien de los sistemas de tratamiento de información.

9.1.7. SEGURIDAD DE LOS RECURSOS, DESPACHOS Y OFICINAS

DEFINICIÓN

La seguridad física debe contemplar las diversas estancias de la entidad como oficinas, despachos y los recursos para el tratamiento de información que estén ubicados en las diversas estancias para evitar amenazas naturales o bien amenazas provocadas por la acción humana o accidentes.

Además, una cuestión a tener en cuenta es la adopción de un puesto de trabajo libre de papeles que contengan datos de carácter personal o información sensible, medios de almacenamiento portátiles y un política de pantalla limpia para reducir los riesgos ante accesos no autorizados (Ej.: exposición de contraseñas de acceso a los sistemas de información), perdida o daño de la información tanto durante como fuera de la jornada laboral.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la existencia de una política respecto a la seguridad física de la entidad (recursos, despachos y oficinas) que, además, contemple directrices de puestos de trabajo despejado de papeles y de medios de almacenamiento extraíbles juntamente con pantalla limpia de información sensible, ya sea, credenciales de acceso a los recursos de tratamiento de la información como la propia información en referencia a datos de carácter personal.

VERIFICACIÓN DE SU CUMPLIMIENTO

No se dispone de una política respecto a la seguridad de los recursos, despachos y oficinas de la propia entidad y, en consecuencia, tampoco tiene en consideración directrices de puestos de trabajo despejados y pantalla limpia de información sensible que pudieran afectar de manera directa o indirecta a los afectados del tratamiento de datos de carácter personal.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá disponer de una política respecto a la seguridad de los recursos, despachos y oficinas de la propia entidad que contemple, además, la adopción de un puesto de trabajo libre de papeles y medios de almacenamiento para reducir riesgos ante accesos no autorizados, pérdida o daño a la información.

RECOMENDACIONES DEL AUDITOR

Es importante aplicar seguridad física en las ubicaciones de la entidad donde se realizan tratamientos de datos de carácter personal especialmente con la finalidad de evitar la exposición de información que pudiera perjudicar a los afectados de los tratamientos.

Para ello, además de utilizar mecanismos de control de acceso a los mismos, es recomendable señalar dichas ubicaciones con distintivos no obvios donde se indique qué funciones se desarrollan en cada una de las ubicaciones. Además, mantener cada uno de los puestos de trabajo despejados de papeles sin medios de almacenamiento extraíbles a la vista de personas no autorizadas y, mantener unos criterios de pantallas limpias de información garantiza que solamente el personal autorizado podrá acceder a la información sensible.

9.1.8. CONTROL DE ACCESO FÍSICO

DEFINICIÓN

El control de acceso dentro de la entidad es una parte fundamental para el tratamiento de datos de personal no autorizado. Cabe destacar que, controlar el acceso no solo se trata de controlar físicamente los accesos sino que además, se debe controlar los accesos a los activos de información.

Para ello, se requiere la realización de una política para el control de acceso para el personal autorizado a acceder físicamente y a tratar la información de la entidad.

Además de la política de control de acceso se deberá considerar la gestión de los derechos de cada usuario autorizado, procedimientos seguros de inicio de sesión, restricciones a las herramientas de configuración de los sistemas y, por último establecer un registro de eventos para obtener evidencias ante anomalías, incidentes o detección de accesos no autorizados.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la existencia del control de acceso físico dentro de las instalaciones de la entidad considerando reglas apropiadas para el control de acceso y, además, derechos y restricciones del personal para acceder a los recursos de la entidad.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de una política para el control de acceso pero no se mantiene actualizada.

La entidad no aplica los criterios establecidos en la presente política de control de acceso físico.

Cuando la entidad trata datos de categoría especial, no dispone de zonas restringidas dotadas de sistemas de apertura mediante llave u otros mecanismos de acceso.

No se mantiene actualizada la relación de personas autorizadas a acceder a las instalaciones donde están ubicados los sistemas de información.

No se registran, de forma manual o automática, los accesos del personal a los sistemas de información.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizada la presente política para hacer frente a los accesos de personal no autorizado a los recursos y sistemas de información de la entidad.

Se deberá aplicar de forma activa la presente política para evitar riesgos en los accesos a los recursos de la entidad.

Cuando la entidad trate datos de categoría especial, deberá disponer de zonas restringidas dotadas de sistemas de apertura mediante llave u otros mecanismos de acceso.

Se deberá mantener actualizada la relación de personas autorizadas a acceder a las instalaciones donde están ubicados los sistemas de información.

Se deberá registrar, de forma manual o automática, los accesos del personal a los sistemas de información.

RECOMENDACIONES DEL AUDITOR

Se deberá tener en consideración en el diseño de la política de control de acceso físico, los criterios para la autorización basados en el ‘Principio de la necesidad de conocer’ y también en la ‘Necesidad de usar’. Además, se deberá tener en cuenta la clasificación de la información, la legislación aplicable, con especial atención al Reglamento General de Protección de Datos de carácter personal y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, los requisitos para la autorización formal de las peticiones de acceso y, por último, se deberá establecer un registro ya sea en formato electrónico o manual de las entradas y salidas del personal.

9.1.9. PROCEDIMIENTOS DE TRATAMIENTOS NO AUTOMATIZADOS

DEFINICIÓN

Debemos destacar tres aspectos fundamentales relativos a los procedimientos de tratamientos no automatizados.

Por un lado, el etiquetado de la información (ya sea información impresa como automatizada) estableciendo unos criterios para determinar el grado de sensibilidad de cada conjunto de información. Para ello, no solamente se etiquetará la información sino que también se deberá etiquetar el propio soporte con distintivos no obvios, fácilmente reconocibles y que estén con acorde con el esquema de clasificación adoptado por la organización.

Por otro lado, la manipulación de la información. Disponer de procedimientos para dicha finalidad reduce la exposición de información de mayor sensibilidad a personal no autorizado. En caso de que la información pueda ser tratada por terceros, establecer criterios para la identificación de la información y facilitar la clasificación de la información para una mejor interpretación de las terceras partes.

Finalmente, cuando la información pueda tratarse fuera de las dependencias de la entidad se deberán aplicar medidas para evitar accesos no autorizados, usos indebidos o deterioros.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de un procedimiento respecto a las operaciones de tratamiento no automatizadas donde se deberá contemplar la existencia de una cultura de etiquetado de la información junto con un procedimiento de manipulación de la información y, en caso de disponer de soportes de almacenamiento, la existencia de un procedimiento para el tránsito de dichos soportes cuando salgan de las dependencias de la entidad.

VERIFICACIÓN DE SU CUMPLIMIENTO

Etiquetado y manipulación de la información

No se dispone de un procedimiento respecto al etiquetado y manipulación de la información y, por tanto, no dispone de un control exhaustivo sobre qué información es tratada en la entidad.

La entidad ha establecido criterios para el archivo de documentos en papel en base al esquema de clasificación de la propia entidad.

El criterio de archivo que ha considerado la entidad es: Documentación inventariada y bajo llave.

Los dispositivos de almacenamiento no disponen de mecanismos que obstaculizen la apertura y, además, no se han adoptado medidas que impiden el acceso a personas no autorizadas.

La documentación es custodiada de manera incorrecta cuando ésta no se encuentra archivada en los dispositivos de almacenamiento, incluso, cuando se encuentran fuera de las dependencias de la entidad.

Soportes físicos en tránsito

Se dispone de una política de seguridad para los soportes de almacenamiento que se encuentren en tránsito para evitar accesos no autorizados, usos indebidos o, simplemente, deterioro.

Aún así, la presente política no se mantiene actualizada.

La entidad no aplica de forma activa la presente política.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Etiquetado y manipulación de la información

Se deberá diseñar e implantar un procedimiento para el etiquetado de la información propiedad de la entidad donde se reflejara los activos de información relacionados ya sea en soporte físico o electrónico y, además, establecer criterios para el archivo de documentos, criterios para la conservación de la documentación en soporte papel y electrónico, mecanismos de seguridad para los dispositivos de almacenamiento teniendo en cuenta cuando se encuentren fuera de las dependencias de la entidad.

Los dispositivos de almacenamiento deberán disponer de mecanismos que obstaculizen la apertura. Se deberán adoptar medidas que impidan el acceso a personas no autorizadas.

La documentación deberá ser custodiada de manera correcta cuando ésta no se encuentre archivada en los dispositivos de almacenamiento, incluso, cuando se encuentren fuera de las dependencias de la entidad.

Soportes físicos en tránsito

Se deberá mantener actualizada la política para evitar accesos no autorizados, usos indebidos o, simplemente, deterioro.

Se deberá implantar la política para que el personal autorizado a la manipulación de soportes de almacenamiento de información de datos de carácter personal esté concienciado de las medidas de seguridad a adoptar en caso que los soportes salgan de las dependencias propiedad de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL.

RECOMENDACIONES DEL AUDITOR

Etiquetado y manipulación de la información

Clasificar y etiquetar la información que trata la entidad es un requisito clave para obtener un control exhaustivo de cual es la información más susceptible ante una amenaza de seguridad.

En el etiquedado de la clasificación para la información en papel se utilizarán distintivos físicos no obvios (Ej.: adhesivos de colores) y para la información contenida en dispositivos electrónicos se utilizarán los metadatos.

Cabe señalar que el uso de etiquetas obvias puede ser contraproducente para la seguridad de la información ya que puede ser identificada facilmente por personal no autorizado y, por tanto, más susceptible de ser robada.

Soportes físicos en tránsito

Tanto si la información es en formato automatizado o no automatizado se deberán usar medidas para proteger los soportes que contengan dicha información. Cuando la información sea de carácter especial (información sensible) se recomienda usar medidas adicionales para asegurar el soporte ya sea mediante cifrado y mecanismos para el acceso solamente a personal autorizado.

9.2. SEGURIDAD INFORMÁTICA

9.2.1. SEGURIDAD EN LOS EQUIPOS INFORMÁTICOS

Procedimientos de operación

DEFINICIÓN

Cuando hablamos de procedimientos de operación nos referimos a un conjunto de procedimientos documentados para desarrollar las actividades asociadas a los sistemas de tratamiento de información tales como procedimiento de encendido y apagado de sistemas, copias de seguridad, mantenimiento de los equipos, gestión de soportes, gestión de centro de procesamientos de datos, gestión del correo y la seguridad de los activos de información.

DATOS, HECHOS Y OBSERVACIONES

Se ha analizado la existencia de un conjunto de procedimientos de operación para las actividades que se vinculen con los recursos de tratamiento y comunicación de la información.

VERIFICACIÓN DE SU CUMPLIMIENTO

Procedimientos de operación

No se ha desarrollado un conjunto de procedimientos de operación vinculadas a los activos de información y relacionados con las operaciones de tratamiento de datos de carácter personal.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá diseñar, y además poner a disposición de todos los usuarios que estén implicados, un conjunto de procedimientos de operación donde se consideren procedimientos como: encendido y apagado de ordenadores, copias de seguridad periódicas, mantenimiento de los equipos informáticos, gestión de los soportes, gestión de las salas de servidores, en caso de existir, gestión del correo electrónico y la seguridad de todos los activos que estén vinculados con los datos de carácter personal principalmente.

RECOMENDACIONES DEL AUDITOR

Se recomienda detallar las instrucciones de cada tarea teniendo en cuenta, principalmente:

- Instalación y configuración de los sistemas de tratamiento de datos.
- La gestión de la información ya sea de carácter automatizado o no.
- Copias de seguridad.
- Contactos de soporte y escalado para el manejo de errores o violaciones de seguridad en los sistemas de tratamiento de información.
- Sincronización de los relojes de todos los sistemas mediante una única fuente precisa de tiempo para garantizar la fiabilidad de los registros generados ante una auditoría, pericial o cualquier otra actividad que precise obtener el tiempo exacto de un suceso.
- Gestión de pistas de auditoría y de la información del registro de eventos del sistema.
- Procedimientos de monitorización de los recursos de la entidad.

Mantenimiento de los equipos propiedad de la organización

DEFINICIÓN

El mantenimiento de los sistemas garantiza una buena seguridad, sobretodo en referencia a la disponibilidad e integridad de la información. Para ello, es recomendable establecer directrices como: la autorización formal del personal responsable de llevar a cabo el mantenimiento de los sistemas, mantener registros ante fallos o incidentes de seguridad y, por último, la verificación de los equipos después de su mantenimiento.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de procedimientos para el mantenimiento de los equipos propiedad de la entidad para asegurar la disponibilidad e integridad de los mismos.

VERIFICACIÓN DE SU CUMPLIMIENTO

No se dispone de un conjunto de procedimientos para el mantenimiento correcto de los equipos informáticos al fin de asegurar la disponibilidad e integridad de los mismos.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá diseñar un conjunto de procedimientos respecto al mantenimiento de los equipos informáticos propiedad de la entidad, mantenerlos actualizados en el tiempo y, además comunicarlos a las personas afectadas que realicen tratamientos de datos de carácter personal.

RECOMENDACIONES DEL AUDITOR

Para la realización de los procedimientos, se deberá tener en consideración, principalmente:

- El mantenimiento de los equipos informáticos será realizado por el personal debidamente autorizado.
- Mantener registros de los fallos ocurridos en los sistemas informáticos, así como también, registros de los mantenimientos realizados ya sean de carácter preventivo o correctivo.
- Cuando se deba realizar el mantenimiento de un equipo informático a través de algún prestador de servicio se deberá borrar la información previamente si contiene datos de categoría especial.
- Una vez finalizado el mantenimiento, ya sea de forma interna o externa a través de un prestador de servicio, se deberá inspeccionar el equipo para verificar que no se ha manipulado malintencionadamente y que funciona de manera correcta.

Retirada de activos fuera de los emplazamientos

DEFINICIÓN

En aquellos casos que los activos de información puedan salir fuera de las dependencias de la entidad se deben realizar determinados procedimientos para que se pueda garantizar la integridad y confidencialidad de la información de la misma manera que cuando se encuentran dentro de las propias instalaciones.

Es por ello, que se deberán realizar autorizaciones formales que permita al personal sacar los activos de información. Además, se puede llevar a cabo un registro del personal autorizado y otro registro para tener evidencias de los activos de información que se encuentran fuera de las instalaciones y cuál es la fecha límite para que el activo se encuentre fuera de las instalaciones.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la existencia de un procedimiento para los activos propiedad de la entidad que salgan fuera de las instalaciones.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de un procedimiento respecto a la salida de activos propiedad de la entidad pero no se mantiene actualizado.

La entidad no aplica de forma activa el presente procedimiento.

La entidad no mantiene actualizada la relación de autorizaciones para sacar los activos fuera de las instalaciones.

SALVEDADES

No existen

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el procedimiento respecto a la salida de activos fuera de la entidad siempre que exista algún cambio en el mismo.

Se deberá aplicar de forma activa el presente procedimiento para evitar que exista un descontrol respecto a los activos propiedad de la entidad y, evitar así, riesgos respecto a la integridad y confidencialidad. Además, disponer de un inventario de activos y mantener un registro de salida de activos reduce el riesgo de fugas de información.

Se deberá mantener actualizada la relación de autorizaciones para sacar fuera de las instalaciones los activos de información.

RECOMENDACIONES DEL AUDITOR

Para mantener un mayor control respecto a los activos que deban sacarse de la entidad, se deberá tener en cuenta:

- Autorización formal para conceder permisos al personal para sacar los activos.
- Registrar fecha y hora de la salida y retorno del activo.
- Establecer limitaciones del tiempo que el activo puede estar fuera de las dependencias.

Además, se puede considerar la realización de inspecciones aleatorias al fin de detectar salidas de activos no autorizadas o bien prevenir la introducción de activos no autorizados.

Se recomienda que, cuando existan introducciones de activos dentro de la entidad, se verifique la procedencia, la propiedad del mismo y, en cualquier caso, inspeccionar el activo en un entorno controlado fuera del área de producción al final de evitar programas potencialmente peligrosos que alteren el funcionamiento normal de la actividad de la empresa.

Eliminación o reutilización segura de los equipos

DEFINICIÓN

Antes de reutilizar o eliminar equipos o medios de almacenamiento, se debería cerciorar que no existe información sensible en los mismos. Para ello, es recomendable llevar a cabo procedimientos de

reutilización o eliminación de los medios de almacenamiento para que no se puedan correr riesgos de fugas de información, principalmente.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la existencia de procedimientos respecto a la eliminación o reutilización segura de los equipos de la entidad.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de procedimientos respecto a la reutilización y eliminación segura de los equipos informáticos y dispositivos de almacenamiento de la entidad.

Aún así, dichos procedimientos no se mantienen actualizados.

Los procedimientos no se están aplicando y no son informados a las personas afectadas.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberán mantener actualizados los procedimientos respecto a la eliminación de equipos siempre que exista algún cambio en los mismos.

Se deberá aplicar de forma activa los presentes procedimientos para evitar el acceso a datos de carácter personal a personas no autorizadas e, incluso, fugas de información.

RECOMENDACIONES DEL AUDITOR

Se debería hacer una inspección de los medios de almacenamiento y equipos informáticos para evaluar si se debe reutilizar o bien destruir cuando se detecten anomalías. En caso de reutilización se aconseja realizar técnicas de sobre escritura segura. Si se decide no reutilizar el dispositivo se utilizarán técnicas de destrucción física segura.

Una eliminación o reutilización no cuidadosa puede afectar a la confidencialidad de la información.

Para más información, consultar apartado *8.1.5 Destrucción y supresión de la información* del documento Medidas y Procedimientos.

Equipos de usuario desatendidos

DEFINICIÓN

Los usuarios deberían asegurarse que se aplican las medidas de seguridad adecuadas cuando los equipos se encuentran desatendidos para evitar, principalmente, riesgos de accesos no autorizados. Algunas de las medidas son: terminar o bloquear sesiones activas de los equipos personales y, también, terminar las sesiones de las aplicaciones o servicios de red cuando ya no sean necesarias.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia y aplicación de un procedimiento para los equipos que se encuentren desatendidos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de procedimientos respecto a los equipos que se encuentren desatendidos.

Pero la entidad no se responsabiliza de mantener dichos procedimientos actualizados cuando existen cambios significativos.

Los procedimientos no se aplican de manera activa y tampoco son comunicados al personal afectado.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberán mantener actualizados los procedimientos respecto a los equipos desatendidos de la entidad siempre que exista algún cambio en los mismos.

Se deberá aplicar de forma activa los procedimientos para evitar el acceso a datos de carácter personal a personas no autorizadas que pudieran conllevar riesgos que afecten a la confidencialidad, integridad e incluso disponibilidad.

RECOMENDACIONES DEL AUDITOR

Algunas de las cuestiones a tener en cuenta para el cumplimiento del presente procedimiento serán:

- Bloquear el equipo en el momento que se desee desatender el mismo y, utilizar mecanismos de seguridad para la verificación de usuarios (uso de contraseñas) para poder continuar trabajando con el equipo.
- Cierre de sesiones de manera automática después de un periodo de inactividad.
- Cerrar las sesiones de usuario, de manera voluntaria, cuando ya no se necesite realizar ninguna tarea durante un periodo largo (Ej.: más de 10min).

Aplicaciones en uso

DEFINICIÓN

Los sistemas operativos, y software en general, deberían estar controlados en todo momento para garantizar la integridad de los mismos.

Para llevar a cabo dichos controles es recomendable que las actualizaciones se realicen por personal debidamente autorizado. Además, cuando se trate de sistemas operativos o software de nueva adquisición deberán superar pruebas exhaustivas de usabilidad y seguridad en un entorno controlado.

Por último, es conveniente tener un registro de auditoría de todas las actualizaciones llevadas a cabo y conservar versiones anteriores como medida de contingencia.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de un procedimiento respecto a la gestión de las aplicaciones y sistemas operativos que utiliza la entidad para obtener un mayor control de los mismos.

VERIFICACIÓN DE SU CUMPLIMIENTO

No se dispone de un procedimiento respecto a la gestión de las aplicaciones y sistemas operativos para obtener un mayor control del software utilizado por la entidad.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá diseñar un procedimiento respecto a la gestión de aplicaciones y sistemas operativos de la entidad para evitar la instalación y uso de programas no admitidos por la entidad. Además, se deberá comunicar a todo el personal involucrado para una correcta gestión de los mismos.

RECOMENDACIONES DEL AUDITOR

La gestión del software de la entidad será llevada a cabo por personal debidamente autorizado por la Dirección.

Una buena práctica es la realización de pruebas de software y sistemas operativos antes de implementarlo en la parte de producción, es decir, antes de usarlo para la actividad normal de la entidad.

Se deberá asegurar que cualquier aplicación o sistema operativo pueda regresar a una versión anterior siempre que exista un funcionamiento anormal de la misma. Para ello, se deberá archivar toda la información oportuna como: detalles de configuración, procedimientos específicos e, incluso, aplicaciones de apoyo.

Llevar a cabo un registro de las actualizaciones permitirá obtener un mayor control de las aplicaciones y sistemas operativos e incluso permitirá detectar equipos afectados ante anomalías de funcionamiento.

Deshabilitar permisos para la instalación y modificación de software y sistemas operativos a usuarios no administradores proporciona un mayor nivel de seguridad ante la información de la entidad y, concretamente, al tratamiento de datos de carácter personal.

Restricciones de aplicaciones

DEFINICIÓN

Toda entidad que realice tratamientos de información a través de medios automatizados, deberá disponer de una estricta política de qué tipo de aplicaciones están permitidas utilizar.

Además, es conveniente conceder permisos para los usuarios para que dispongan del mínimo privilegio en los propios sistemas. Prohibir la instalación de software y, solamente conceder permisos para las actualizaciones de las aplicaciones permitidas reduce el riesgo de fugas de información, pérdidas de integridad o bien otros incidentes que afecten a la seguridad de la información como accesos no autorizados o la introducción de programas maliciosos (Ej.: virus, troyanos, *keyloggers*, *rootkits*,…).

DATOS, HECHOS Y OBSERVACIONES

Se ha analizado la existencia de un procedimiento respecto a las restricciones que se le aplican al software de la entidad teniendo en cuenta también las restricciones en los sistemas operativos.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de un procedimiento para la aplicación de restricciones en referencia al software y sistemas operativos de la entidad.

La entidad no actualiza el presente procedimiento cuando existe algun cambio sustancial.

La entidad no está comprometida en la aplicación del presente procedimiento y a comunicar a todo el personal involucrado como llevar a cabo dicho procedimiento.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el procedimiento respecto a la aplicación de restricciones en referencia al software y sistemas operativos de la entidad.

Se deberá aplicar de forma activa el presente procedimiento para hacer frente la introducción de vulnerabilidades en los sistemas, pérdida de integridad o bien otros incidentes que afecten a la seguridad de la información como accesos no autorizados o la introducción de programas maliciosos (Ej.: virus, troyanos, *keyloggers*, *rootkits*,…).

Además, se deberá comunicar a todo el personal involucrado como llevar a cabo dicho procedimiento.

RECOMENDACIONES DEL AUDITOR

La gestión de las aplicaciones del software y de los sistemas operativos deberá estar autorizada bajo la Dirección de la entidad y, principalmente recaerá dicha autorización al administrador (o administradores) de sistemas. En caso de no disponer de ésta figura dentro de la entidad, se pueden establecer permisos a los propios usuarios aplicando el principio de menor privilegio.

Gestión de la seguridad en las redes de comunicación

DEFINICIÓN

Las redes de comunicación de la entidad son un punto débil donde se puede producir fugas de información. Para ello, es recomendable establecer una política (o conjunto de procedimientos) donde se detallen, entre otras cuestiones, las autorizaciones de personal o aplicaciones para el uso de las redes, los mecanismos de autenticación a la red y, además, si se requiere cifrado para las transmisiones de información.

Otra cuestión a tener en cuenta es la segregación de las redes (si se requiere) para separar de manera lógica determinados servicios, información, departamentos, entre otros.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar la existencia de un conjunto de procedimientos basados en la seguridad de las redes de comunicación para proteger la información que trata la entidad frente accesos no autorizados o fugas de información.

VERIFICACIÓN DE SU CUMPLIMIENTO

La entidad dispone de un conjunto de procedimientos de gestión de la seguridad en las redes de comunicación.

Aun así, los procedimientos no son mantenidos actualizados cuando existen cambios sustanciales que afecten a los procedimientos.

La entidad no está comprometida activamente a llevar a cabo los procedimientos ni a comunicarlos al personal afectado.

SALVEDADES

No existen

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el conjunto de procedimientos respecto a la gestión de la seguridad en las redes de comunicación siempre que exista algún cambio en los mismos.

Se deberá aplicar de forma activa el presente conjuntos de procedimientos para evitar accesos no autorizados en los sistemas de información, riesgos de fugas de información, etc. Además, será conveniente comunicar la aplicación de dichos procedimientos a todo el personal afectado.

RECOMENDACIONES DEL AUDITOR

Algunas de las recomendaciones para maximizar la seguridad en las redes de comunicación son:

- Establecer responsabilidades para la gestión de las redes de comunicación.
- Aplicar mecanismos para hacer frente accesos no autorizados.
- Establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que transitan a través de las redes, sobretodo, cuando se tratan datos de categoría especial.
- Monitorización de las comunicaciones y registro de eventos para obtener evidencias en caso de violaciones de seguridad.
- Conexiones restringidas a los sistemas de información.
- Separar las redes en función de los servicios de información, grupos de usuarios y sistemas de información. Además, para las redes inalámbricas, se deberá tener un trato especial para las configuraciones de seguridad.
- Cuando existan proveedores de servicios con acceso a la información de la entidad, se deberá especificar en los acuerdos o contratos de prestación de servicios las medidas de seguridad que deberá seguir el prestador.

Mensajería electrónica

DEFINICIÓN

La información intercambiada mediante mensajería electrónica debe estar debidamente protegida. Para ello, es necesario determinar un conjunto de acciones para garantizar la integridad y confidencialidad de la misma. Algunas de estas acciones son: establecer protección contra accesos no autorizados a las aplicaciones de mensajería, asegurar la fiabilidad y disponibilidad del servicio, consideraciones legales tales como la firma electrónica para aquella información considerada sensible en la clasificación de la información establecida por la entidad, o bien, mayores niveles de protección contra accesos no autorizados cuando se intercambie información desde redes públicas.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de una política o procedimiento respecto a la información que es comunicada a través de mensajería electrónica, ya sea mediante correo electrónico o mensajería instantánea.

VERIFICACIÓN DE SU CUMPLIMIENTO

La entidad dispone de una política o procedimiento respecto a la seguridad del uso en mensajería electrónica.

Cuando existe algun cambio significativo dentro de la organización que afecte a la política o procedimiento de mensajería electrónica no se mantiene actualizado.

La entidad no lleva a cabo la presente política o procedimiento y, tampoco, se le ha comunicado al personal involucrado.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado la política o procedimiento respecto a la seguridad del uso en mensajería electrónica siempre que exista algún cambio significativo.

Se deberá aplicar de forma activa la presente política o procedimiento y comunicarlo al personal que utilice herramientas de mensajería instantánea.

RECOMENDACIONES DEL AUDITOR

Se recomienda establecer protección frente a accesos no autorizados, modificación o denegación del servicio conforme a la clasificación de la información adoptado por la entidad.

Se deberá asegurar, principalmente, el correcto direccionamiento y transporte del mensaje, además de la disponibilidad y fiabilidad del servicio.

Cuando se traten datos de categoría especial, se deberá utilizar mecanismos para ocultar el contenido del mensaje mediante cifrado como por ejemplo, haciendo uso de certificados digitales.

Además, para el tratamiento de datos de categoría especial, se evitará en la medida de lo posible, hacer uso de herramientas de mensajería electrónica en redes públicas. Cuando no se pueda utilizar una alternativa, los mensajes deberán estar encriptados para evitar fugas de información.

9.2.2. POLÍTICAS DE SEGURIDAD EN ENTORNOS DE DESARROLLO

DEFINICIÓN

Por la actividad que realiza la entidad, considerar una política de seguridad en entornos de desarrollo de software es de suma importancia ya que abarca varios factores que se deben tener en consideración para no estar expuestos ante riesgos que afecten a la integridad, confidencialidad e, incluso, disponibilidad de la información.

Una parte básica a tener en cuenta es la separación de los entornos de desarrollo (y prueba) de la de producción (u operación) para reducir los riesgos de accesos no autorizados.

También, se debe tener en consideración el diseño de procedimientos de actuación para el desarrollo de software y sistemas.

Así mismo, los datos que sean tratados en entornos de prueba se deben seleccionar de manera cuidadosa además de estar protegidos y controlados con especial autorización formal cuando sean tratados los datos de entornos de producción.

DATOS, HECHOS Y OBSERVACIONES

La actividad de la organización no está relacionada con el desarrollo de software ni sistemas de información, por tanto, el presente apartado no le es de aplicación.

VERIFICACIÓN DE SU CUMPLIMIENTO

No proceden.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

No proceden.

9.2.3. ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIÓN

DEFINICIÓN

Para el acceso a datos a través de redes de comunicación se debe establecer una política y un conjunto de procedimientos de actuación para garantizar principalmente el acceso a personal no autorizado. Para ello es recomendable establecer una política de control de acceso donde se tenga en consideración las limitaciones y los permisos establecidos a los activos de información.

Además, para el acceso a las redes, ya sean cableadas o mediante redes inalámbricas, también se deberán aplicar controles de acceso y permisos únicamente al personal que tenga deba tener acceso.

Los mecanismos para la autenticación de los usuarios deberán ser adecuados conforme al esquema de clasificación de la información establecido por la entidad. Además, es recomendable configurar un registro de eventos donde se puedan registrar excepciones, intentos de acceso fallidos o cualquier evento de seguridad de la información.

Por último, se deberá tener en consideración, también, el uso de acuerdos de confidencialidad, ya sea para terceros que presten servicios a la propia entidad o bien para el personal interno.

DATOS, HECHOS Y OBSERVACIONES

EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL no dispone de accesos remotos a los sistemas de información propiedad de la entidad. En el momento que decida autorizar accesos remotos, ya sea a personal interno o bien a un tercero, deberá comunicarlo a PROFESSIONAL GROUP CONVERSIA, SLU.

VERIFICACIÓN DE SU CUMPLIMIENTO

No procede.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No proceden.

RECOMENDACIONES DEL AUDITOR

No proceden.

9.2.4. RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE UBICACIÓN DE LOS SISTEMAS DE INFORMACIÓN

DEFINICIÓN

Cuando existe la necesidad de poder realizar tratamientos de información desde fuera de las dependencias de la entidad, se deben aplicar ciertos criterios de seguridad para evitar accesos no autorizados y, además, garantizar la integridad de la información a través de mecanismos de seguridad.

Parra ello, se debe diseñar una política de dispositivos móviles que tenga en consideración requisitos de protección física, restricciones de instalación de software, controles de acceso y técnicas criptográficas para el tránsito y almacenamiento de la información principalmente.

Además, para las tareas desde fuera de las dependencias (teletrabajo) se debe tener en consideración una política donde refleje, entre otras medidas: la existencia de medidas de seguridad física en el entorno de teletrabajo, los requisitos frente a software malicioso, mecanismos de seguridad contra accesos no autorizados.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de una política o bien procedimento respecto al régimen que debe adoptar el personal que realice tareas fuera de los locales de ubicación de los sistemas de información y, además, la seguridad mínima que deben tener los equipos cuando salgan de las propias instalaciones.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de una política o procedimiento respecto al régimen de trabajo fuera de las instalaciones propiedad de la entidad.

Aún así, la política o procedimiento no se mantiene actualizado cuando existe un cambio significativo.

La entidad no ha implementado la política o procedimiento y, a su vez, no ha hecho efectiva la comunicación a todo el personal involucrado.

Existe una relación actualizada de las autorizaciones del personal que puede tratar datos de carácter personal fuera de las dependencias de la entidad.

EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL no almacena categoría especiales de datos en los dispositivos portátiles para trabajar fuera de las dependencias principales.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizada la política o procedimiento siempre que exista un cambio significativo que afecte a la presente política.

Se deberá implementar la política o procedimiento y, comunicar a todo el personal autorizado a realizar tareas fuera de las dependencias de la entidad.

RECOMENDACIONES DEL AUDITOR

La presente política deberá adoptar medidas de seguridad para la protección en el uso de dispositivos móviles cuando se encuentren en entornos desprotegidos. Para ello, se deberá tener en cuenta principalmente:

- Autorización formal de los dispositivos y usuarios autorizados para realizar tareas fuera de las instalaciones.
- Registro de entrada y salida de los dispositivos móviles que se encuentre fuera de las instalaciones, juntamente con la protección física y lógica que deberá adoptar, la restricciones de aplicaciones y conexiones a realizar, controles de acceso, técnicas criptográficas para las comunicaciones, protección contra software malicioso y, además, habilitar el bloqueo/borrado remoto y la realización de copias de seguridad periódicas.
- Aplicar medidas de seguridad adecuadas para la protección de la información accedida en los sistemas de información que se ubiquen en las instalaciones de la entidad.

9.2.5. GESTIÓN DE USUARIOS

DEFINICIÓN

Gestionar los usuarios de la entidad debe ser una consideración de suma importancia ya que, según los permisos concedidos, los riesgos pueden tener mayor o menor impacto a la información propiedad de la entidad.

Para realizar una efectiva gestión de usuarios se debe tener en cuenta, principalmente:

- El alta y baja del usuario teniendo en cuenta que, para el alta, se deberá proporcionar una cuenta de usuario única por empleado (siempre que sea posible) y, para la baja, inhabilitar/eliminar de inmediato la cuenta cuando ya no sea necesaria.
- Diseñar un procedimiento para la gestión de privilegios de los usuarios siempre en base a la 'necesidad de uso'.
- Realizar un proceso formal de autorización, y requiriendo la firma del usuario, a través de un compromiso de confidencialidad.

DATOS, HECHOS Y OBSERVACIONES

Se ha analizado la existencia de una política o procedimiento respecto a la gestión de los usuarios que forman parte de la entidad para hacer frente riesgos de accesos no autorizados.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de una política pero no se mantiene actualizado cuando existe un cambio significativo.

La entidad no ha implementado de forma activa la presente política y no ha hecho efectiva la comunicación a todo el personal que dispone de una cuenta de usuario para el acceso a los sistemas de información.

Cada usuario accede a los sistemas de información mediante mecanismos de autenticación. Además, los mecanismos de autenticación son unipersonales.

El mecanismo para el acceso a los sistemas de información utilizado por la entidad es:

Identificador y contraseña

La entidad establece una limitación del acceso a los sistemas de información al personal no autorizado.

La entidad dispone de una relación de los usuarios autorizados al acceso a los sistemas de información y, además, la mantiene actualizada.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizada la política siempre que exista un cambio significativo.

Se deberá implementar de forma activa la presente política y, a su vez, se deberá hacer efectiva la comunicación a todo el personal que disponga de cuenta de usuario para acceder a los sistemas de información.

RECOMENDACIONES DEL AUDITOR

La creación de una política de gestión de usuarios debe ser una parte fundamental para toda entidad que trate información de manera automatizada.

Para realizar una política de manera eficiente existen varios aspectos que se deben tener en cuenta:

Se considerarán los procedimientos a seguir para la creación y revocación de las cuentas de usuario donde se hace especial hincapié en la autorización formal por parte de la Dirección de la creación de las cuentas, el uso de identificadores únicos para cada usuario evitando así redundancias de usuarios y revisiones periódicas de las cuentas habilitadas.

El personal al cual se le conceda una autorización para poseer un usuario del sistema de información deberá firmar un compromiso de confidencialidad y responsabilizarse de custodiar la información secreta para el acceso a los sistemas de información. Dicha información secreta de autenticación, deberá cambiarse antes de hacer el primer uso de la cuenta de usuario.

El personal encargado de administrar los sistemas de información deberá realizar revisiones periódicas de las cuentas que se han dado de alta para verificar si la cuenta sigue siendo útil y, en tal caso, revisar los derechos de acceso siempre persiguiendo el principio de menor privilegio.

Los derechos de acceso concedidos se deberán revocar cuando finalice el contrato o el acuerdo establecido entre las partes.

En el caso que se utilicen herramientas para la generación de contraseñas se deberá verificar, antes del primer uso, que la herramienta puede generar contraseñas siguiendo las recomendaciones de generación de contraseñas seguras.

9.2.6. INVENTARIO DE APLICACIONES INFORMÁTICAS

DEFINICIÓN

La instalación incontrolada de aplicaciones en los equipos informáticos puede conllevar a maximizar vulnerabilidades en los mismos y, en consiguiente, fugas de información, pérdida de integridad u otros incidentes respecto a la seguridad de la información.

Es por ello que realizar un inventario de las aplicaciones que tienen derecho a acceder o instalar los propios usuarios es otra de las cuestiones a tener en cuenta dentro de la entidad. Dentro de las instalaciones que puede realizar el propio personal se incluyen actualizaciones y parches de seguridad.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de un inventario de las aplicaciones informáticas que la Dirección de la entidad ha autorizado dentro de la organización.

VERIFICACIÓN DE SU CUMPLIMIENTO

No se dispone de un procedimiento actualizado relativo al inventario de aplicaciones que utiliza la entidad.

La entidad no aplica de forma activa el procedimiento relativo al inventariado relativo a las aplicaciones que utiliza la propia entidad.

La entidad no dispone de una relación actualizada de las aplicaciones permitidas para el tratamiento de datos de carácter perosnal.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el procedimiento relativo al inventario de aplicaciones de la organización.

La entidad deberá aplicar de forma activa el procedimiento relativo al inventariado relativo a las aplicaciones que utiliza la propia entidad

La entidad deberá disponer de una relación actualizada de las aplicaciones permitidas para el tratamiento de datos de carácter perosnal.

RECOMENDACIONES DEL AUDITOR

La introducción incontrolada de aplicaciones dentro de la entidad puede conllevar la introducción de vulnerabilidades y provocar que la información se vea amenazada por fugas de información o bien perdida de la integridad.

9.2.7. GESTIÓN DE SOPORTES

DEFINICIÓN

Para la gestion de soportes es recomendable diseñar e implantar un conjunto adecuado de procedimientos para el etiquetado, de la información y los activos relacionados, en acorde con el esquema de clasificación adoptado por la propia organización (véase apartado 5 Recursos protegidos del documento *Medidas y Procedimientos*).

Éstos procedimientos de etiquetado contemplan la información y los activos relacionados tanto en soporte físico como electrónico y proporcionan directrices sobre dónde y cómo se vinculan las etiquetas considerando como se accede a la información o, bien, como se tratan los activos de información dependiendo del tipo de soporte.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de un procedimiento respecto a la gestión de los soportes propiedad de la entidad.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de un procedimiento respecto a la gestión de los soportespero no se mantiene actualizado.

La entidad no aplica de forma activa el presente procedimiento y no ha hecho efectiva la comunicación a todo el personal involucrado.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el procedimiento respecto a la gestión de los soportes siempre que exista algún cambio en los mismos.

Se deberá aplicar de forma activa el presente procedimiento.

RECOMENDACIONES DEL AUDITOR

Cuando mencionamos soportes, nos podemos referir tanto a soportes físicos para información no automatizada como a soportes electrónicos. La gestión de dichos soportes parte principalmente de la clasificación de la información establecida por la entidad en la cual se deberán etiquetar los soportes físicos con distintivos no obvios y, para los soportes electrónicos mediante metadatos.

9.2.8. PROCEDIMIENTO DE COPIAS DE SEGURIDAD Y RECUPERACIÓN

DEFINICIÓN

La realización de copias de seguridad debe garantizar en todo momento la reconstrucción de la información respaldada en el estado en que se encontraban cuando se realizó la copia.

En caso que la información respaldada sea considerada sensible según el esquema de clasificación de la entidad, dicha copia deberá ser resguardada fuera de las instalaciones principales. Así mismo, se recomienda realizar el respaldo de forma cifrada.

Para la realizacion del procedimiento de copias de seguridad se deberá tener en consideración la creación de registros precisos de las copias así como el procedimiento de recuperación. Además, la frecuencia de las copias y la extensión de cada una de ella (incrementales o totales).

Finalmente, las copias de respaldo deberán poseer protección física ante cualquier riesgo que pudiera deribar pérdida de información en el manipulado de las copias.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de un procedimiento para la realización de las copias de seguridad y recuperación de la información.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha diseñado el procedimiento para la realización de copias de seguridad y recuperación de la información pero no se mantiene actualizado cuando existe algun cambio sustancial.

La entidad no lleva a cabo de forma activa el procedimiento y no lo ha comunicado al personal afectado.

Las copias de seguridad de los datos de carácter personal se realizan en:

- Servidor de copias de seguridad

- En la nube (Cloud computing)

La ejecución de estos procesos se realiza con una frecuencia:

- Diaria

Las copias de seguridad se almacenan en:

- Una ubicación diferente de las dependencias principales

Las copias de seguridad que contienen datos de categoría especial no se guardan dentro de las propias instalaciones de la entidad.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el procedimiento respecto a las copias de seguridad y recuperación cuando exista algún cambio sustancial.

Se deberá aplicar de forma activa el presente procedimiento para evitar la pérdida de información ante una violación de la seguridad. En caso de violación en la seguridad, se deberá reflejar, también, el procedimiento de recuperación de la información.

RECOMENDACIONES DEL AUDITOR

Las copias de seguridad deberían contemplar la propia información tratada por la entidad y, además, los sistemas de información deberían tener su propio respaldo.

Para el el diseño de las copias de seguridad se debería considerar principalmente:

- La creación de registros de las copias así como los procedimientos a seguir deben estar bien documentados.
- La frecuencia de las copias de seguridad deben reflejar los requisitos del negocio y a la criticidad de la información. Se recomienda una frecuencia minima semanal.
- Para los datos de categoria especial, las copias de seguridad se deben guardar en un emplazamiento alejado de los sistemas de información para resguardarse de un incidente en el emplazamiento principal.
- Además, para los datos sensibles, se deben aplicar mecanismos de cifrado en las copias de seguridad.
- Se debe verificar el buen funcionamiento de la herramienta de copias de seguridad, los propios soportes de almacenamiento y, además, si el procedimiento sigue siendo el adecuado o debe realizarse alguna modificación.

9.2.9. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

DEFINICIÓN

La política criptográfica resulta necesaria para maximizar los beneficios y reducir los riesgos (en especial a la información sensible), así como evitar un uso inadecuado o incorrecto de la información tratada.

Al implantar la política de controles criptográficos en la organización, se debería tener en cuenta las regulaciones y restricciones nacionales que puedan resultar aplicables al uso de técnicas criptográficas en las distintas partes del mundo, así como a las cuestiones relativas al flujo transfronterizo de información cifrada.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de una política de controles criptográficos para el tratamiento de datos personales de categoría especial.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha diseñado una política para los controles criptográficos

pero no se mantiene actualizada cuando existe un cambio significativo en la presente política.

La entidad no ha implementado la presente política y, a su vez, no ha hecho efectiva la comunicación de la misma a todo el personal involucrado.

La entidad no realiza envíos telemáticos de datos especialmente protegidos o confidenciales.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado la política respecto a los controles criptográficos siempre que exista algún cambio significativo en los mismos.

Se deberá aplicar de forma activa la presente política para evitar el acceso a datos de carácter personal a personas no autorizadas, fugas de información o bien evitar la lectura de la misma cuando transita por

redes no confiables, principalmente. Además, se deberá comunicar la presente política a todo el personal involucrado.

RECOMENDACIONES DEL AUDITOR

Teniendo en cuenta como base el análisis de los riesgos, se deberá identificar el nivel de protección mínimo identificando el tipo, fortaleza y calidad del alogaritmo de cifrado necesario.

La política sobre el uso de controles criptográficos deberá reflejar qué tipo de control criptográfico debe aplicarse, para qué finalidad y en qué procesos del negocio se aplican.

Igualmente, la política deberá constar la protección y duración de las claves de cifrado.

Una gestión adecuada de las claves privadas requiere procesos seguros de generación, almacenamiento, archivo, recuperación, distribución, retirada y destrucción de las propias claves criptográficas. Para ello, es conveniente que los sistemas de generación de claves cuenten con protección física.

También deberá tenerse en cuenta las claves públicas para determinados procesos del negocio. Dichas claves son expedidas por una autoridad de certificación.

9.3. SEGURIDAD EN LA RELACIÓN CON TERCEROS

DEFINICIÓN

Las relaciones con terceras partes deben garantizar la seguridad de la información de la misma manera que se garantiza cuando la información se encuentra dentro de las dependencias de la entidad. Es por ello que se debe realizar un conjunto de acciones con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de los datos.

Como se ha comentado en el párrafo anterior, para garantizar la seguridad de la información se deberá tener en cuenta:

- Políticas y procedimientos para el intercambio de información.
- Realización de acuerdos de intercambio de información.
- Realización de acuerdos de confidencialidad o no revelación.
- Políticas de seguridad de la información en las relaciones con los proveedores.
- Requisitos de seguridad en contratos con terceros.

DATOS, HECHOS Y OBSERVACIONES

Se ha verificado la existencia de un conjunto de políticas, procedimientos y controles para la protección de los datos de carácter personal cuando se usen todo tipo de recursos de comunicación como la mensajería instantánea, fax, voz o video.

La garantia de una protección fiable para aquella información y medios físicos en tránsito mediante acuerdos de confidencialidad con terceras partes o personal interno.

Además, también se ha verificado la existencia de un conjunto de requisitos que deben cumplir los proveedores ante el acceso a las instalaciones donde se realizan tratamientos de datos de carácter personal.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se disponen de políticas, procedimientos y acuerdos para las relaciones con terceras partes para la protección del intercambio de información de datos de carácter personal.

La entidad no mantiene actualizadas las políticas, procedimientos y acuerdos cuando existen cambios significativos.

Además, la entidad no ha implementado dichas políticas, procedimientos y acuerdos y, a su vez, tampoco ha hecho efectiva la comunicación a todo el personal involucrado.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberán mantener actualizadas las políticas, procedimientos y acuerdos respecto a las relaciones con terceras partes siempre que exista algún cambio en los mismos.

Se deberán aplicar de forma activa las presentes políticas, procedimientos y acuerdos para garantizar una protección fiable cuando existan intercambios de información con terceras partes.

RECOMENDACIONES DEL AUDITOR

La información tratada por la entidad debe estar asegurada durante todo el ciclo de vida de la misma desde su recabado hasta su destrucción. La seguridad es una parte fundamental cuando los datos son tratados por terceras personas o, bien, cuando estos son intercambiados con terceras personas

Para garantizar la integridad, confidencialidad y disponibilidad de la información, la entidad debe asegurarse que la información es tratada con las mismas garantías que lo hace el Responsable del tratamiento mediante políticas, procedimientos y acuerdos.

Para más información, consultar apartado *8.4 Seguridad en la relación con terceros* del documento Medidas y Procedimientos.

9.4 GESTIÓN DE INCIDENCIAS Y VIOLACIONES DE SEGURIDAD DE LOS DATOS

DEFINICIÓN

Realizar una adecuada gestión y notificación de incidencias y violaciones de seguridad de los datos mediante la aplicación de procedimientos.

“Artículo 33. Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El Encargado del Tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34. Comunicación de una violación de la seguridad de los datos personales al Interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos

personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de cumplimiento respecto a la gestión de las violaciones de seguridad en cumplimiento con el Reglamento General de Protección de Datos, así como de la existencia e implantación de procedimientos para gestionar los incidentes de seguridad.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se dispone de un procedimiento o conjunto de procedimientos para la gestión de incidentes o violaciones de seguridad.

La entidad no mantiene actualizado el procedimiento o conjunto de procedimientos cuando existen cambios significativos.

Además, la entidad no ha implementado dicho procedimiento y, a su vez, tampoco ha hecho efectiva la comunicación a todo el personal involucrado.

Se ha verificado la inexistencia de incidentes o violaciones de seguridad.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

Se deberá mantener actualizado el procedimiento o conjunto de procedimientos siempre que exista algún cambio significativo.

Se deberá aplicar de forma activa el presente procedimiento o conjunto de procedimientos además de comunicarlo a todo el personal involucrado.

RECOMENDACIONES DEL AUDITOR

Para garantizar una respuesta rápida, efectiva y adecuada respecto a los incidentes o violaciones de seguridad es necesario establecer responsabilidades e implementar procedimientos de actuación.

Todo el personal involucrado en el tratamiento de datos de carácter personal, ya sean empleados de la propia entidad como terceros, deberían conocer su responsabilidad de realizar la comunicación respecto a cualquier evento en referencia a la seguridad de la información mediante un canal de gestión adecuado y, además, registrarlo.

Los incidentes de seguridad de la información deberían ser analizados y posteriormente decidir si son clasificados realmente como un incidente de seguridad. Si se dictamina que es un incidente de seguridad

debería establecerse mecanismos de contingencia para reducir la probabilidad y gravedad del incidente para un futuro.

Adicionalmente, la entidad debería dictaminar si la continuidad de seguridad de la información queda dentro del proceso de continuidad del negocio o bien dentro del proceso de recuperación de desastres. Para ello, la entidad debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar un nivel adecuado durante una situación adversa.

10. RESUMEN DE NO CONFORMIDADES Y PROPUESTA DE MEDIDAS CORRECTORAS

A modo de resumen, se enumeran las no conformidades observadas según lo estipulado en la normativa de Protección de Datos de Carácter Personal, así como las medidas correctoras recomendadas.

A continuación, con el objeto de determinar de una forma gráfica la situación de las no conformidades identificadas en EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL, se establece la siguiente correlación para diferenciar el grado de no conformidad:

TIPO DE NO CONFORMIDAD	DESCRIPCIÓN
Recomendaciones	
No conformidad Leve	
No conformidad Grave	
No conformidad muy Grave	

8.1. PRINCIPIOS RELATIVOS AL TRATAMIENTO		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
LOS DATOS SE CONSERVAN MÁS TIEMPO DEL INFORMADO EN EL MOMENTO DE LA RECOGIDA DE LOS DATOS	ALMACENAR O CUSTODIAR LOS DATOS EL PLAZO INFORMADO EN EL MOMENTO DE LA RECOGIDA DE LOS DATOS	
EL PROCEDIMIENTO PARA LA SUPRESIÓN DE LOS DATOS NO ES ADECUADO	REVISAR LA ADECUACIÓN DEL PROCEDIMIENTO PARA LA SUPRESIÓN DE LOS DATOS	

8.2. RESPONSABILIDAD PROACTIVA (ACCOUNTABILITY)		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
NO SE HAN CORREGIDO LAS NO CONFORMIDADES DETECTADAS EN LA ANTERIOR AUDITORÍA	SE ACONSEJA IMPLEMENTAR LAS MEDIDAS CORRECTORAS PROPUESTAS EN LAS AUDITORÍAS ANTERIORES	

8.3. LICITUD DEL TRATAMIENTO		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
CUANDO LA BASE LEGÍTIMA DEL TRATAMIENTO SEA EL CONSENTIMIENTO, NO SE PUEDE ACREDITAR LA OBTENCIÓN DEL CONSENTIMIENTO DE LOS INTERESADOS	DISPONER DE DOCUMENTOS QUE ACREDITEN LA OBTENCIÓN DEL CONSENTIMIENTO DE LOS INTERESADOS PARA EL TRATAMIENTO DE SUS DATOS	

8.5. DERECHOS DE LOS INTERESADOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO

NO SE HA IMPLANTADO UN PROCEDIMIENTO ADECUADO PARA LA ATENCIÓN DEL DERECHO DE ACCESO	DISEÑAR E IMPLEMENTAR UN PROCEDIMIENTO ADECUADO PARA ATENDER EL EJERCICIO DEL DERECHO DE ACCESO	
NO SE HA IMPLANTADO UN PROCEDIMIENTO ADECUADO PARA LA ATENCIÓN DEL DERECHO DE RECTIFICACIÓN	DISEÑAR E IMPLEMENTAR UN PROCEDIMIENTO ADECUADO PARA ATENDER EL EJERCICIO DEL DERECHO DE RECTIFICACIÓN	
NO SE HA IMPLANTADO UN PROCEDIMIENTO ADECUADO PARA LA ATENCIÓN DEL DERECHO DE SUPRESIÓN	DISEÑAR E IMPLEMENTAR UN PROCEDIMIENTO ADECUADO PARA ATENDER EL EJERCICIO DEL DERECHO DE SUPRESIÓN	
NO SE HA IMPLANTADO UN PROCEDIMIENTO ADECUADO PARA LA ATENCIÓN DEL DERECHO DE LIMITACIÓN	DISEÑAR E IMPLEMENTAR UN PROCEDIMIENTO ADECUADO PARA ATENDER EL EJERCICIO DEL DERECHO DE LIMITACIÓN	
NO SE HA IMPLANTADO UN PROCEDIMIENTO ADECUADO PARA LA ATENCIÓN DEL DERECHO DE PORTABILIDAD	DISEÑAR E IMPLEMENTAR UN PROCEDIMIENTO ADECUADO PARA ATENDER EL EJERCICIO DEL DERECHO DE PORTABILIDAD	
NO SE HA IMPLANTADO UN PROCEDIMIENTO ADECUADO PARA LA ATENCIÓN DEL DERECHO DE OPOSICIÓN	DISEÑAR E IMPLEMENTAR UN PROCEDIMIENTO ADECUADO PARA ATENDER EL EJERCICIO DEL DERECHO DE OPOSICIÓN	

8.8. PRESTACIÓN DE SERVICIOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
EL ENCARGADO DE TRATAMIENTO NO SE SELECCIONA DE MANERA ADECUADA	ELEGIR UN ENCARGADO DEL TRATAMIENTO QUE OFREZCA GARANTÍAS SUFICIENTES PARA APLICAR MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS	
NO EXISTE UN RELACIÓN DE LOS ENCARGADOS DEL TRATAMIENTO	ESTABLECER UNA RELACIÓN ACTUALIZADA DE LOS ENCARGADOS DEL TRATAMIENTO	

9.1. SEGURIDAD FÍSICA

PROTECCIÓN FRENTE AMENAZAS AMBIENTALES		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
NO SE DISPONE DE UN POLÍTICA/PROCEDIMIENTO FRENTE A LAS AMENAZAS AMBIENTALES	SE DEBERÁ DISPONER DE UNA POLÍTICA O PROCEDIMIENTO FRENTE AMENAZAS AMBIENTALES PARA EVITAR DESASTRES NATURALES, ACCIDENTES O FALLOS PROVOCADOS POR LA ACCIÓN HUMANA	

PUNTOS DE ACCESO		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
EL PROCEDIMIENTO RESPECTO A LOS PUNTOS DE ACCESO DE LA ENTIDAD NO SE MANTIENE ACTUALIZADO	SE DEBERÁ MANTENER ACTUALIZADO EL PROCEDIMIENTO SIEMPRE QUE EXISTA UN CAMBIO QUE AFECTE A LOS PUNTOS DE ACCESO	
EL PROCEDIMIENTO RESPECTO A LOS PUNTOS DE ACCESO NO SE HA IMPLEMENTADO	SE DEBERÁ ALICAR DE FORMA ACTIVA PARA EVITAR EL ACCESO A PERSONAS NO AUTORIZADAS E, INCLUSO, EVITAR LA RECEPCIÓN DE MATERIAL NO DESEADO	

UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
EL PLAN PARA LA COLOCACIÓN DE EQUIPOS PARA EL TRATAMIENTO DE INFORMACIÓN NO SE MANTIENE ACTUALIZADO	SE DEBERÁ MANTENER ACTUALIZADO EL PLAN PARA MINIMIZAR RIESGOS DE PÉRDIDA, DAÑO, ROBO O CUALQUIER OTRO COMPROMISO DE LOS ACTIVOS DE INFORMACIÓN	
EL PLAN PARA LA COLOCACIÓN DE EQUIPOS PARA EL TRATAMIENTO DE INFORMACIÓN NO SE HA IMPLEMENTADO	SE DEBERÁ IMPLEMENTAR EL PLAN PARA MINIMIZAR RIESGOS DE PÉRDIDA, DAÑO, ROBO O CUALQUIER OTRO COMPROMISO DE LOS ACTIVOS DE INFORMACIÓN	

SUMINISTROS EN LOS EQUIPOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
LA POLÍTICA RESPECTO A LAS INSTALACIONES DE SUMINISTRO NO SE MANTIENE ACTUALIZADO	SE DEBERÁ MANTENER ACTUALIZADA LA POLÍTICA RESPECTO A LAS INSTALACIONES DE SUMINISTRO PARA EVITAR FALLOS DE ALIMENTACIÓN E INTERRUPCIÓN DE LAS COMUNICACIONES	
LA POLÍTICA RESPECTO A LAS INSTALACIONES DE SUMINISTRO NO SE HA IMPLANTADO	SE DEBERÁ APLICAR LA POLÍTICA RESPECTO A LAS INSTALACIONES DE SUMINISTRO PARA EVITAR FALLOS DE ALIMENTACIÓN E INTERRUPCIÓN DE LAS COMUNICACIONES	

PROTECCIÓN EN EL CABLEADO		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
NO SE DISPONE DE UNA POLÍTICA/PROCEDIMIENTO RESPECTO A LA PROTECCIÓN EN EL CABLEADO	SE DEBERÁ DISPONER DE UNA POLÍTICA/PROCEDIMIENTO RESPECTO A LA PROTECCIÓN EN EL CABLEADO PARA EVITAR RIESGOS DE INTERFERENCIAS, INTERCEPTACIONES O DAÑOS FÍSICOS EN LOS MISMOS	

GESTIÓN DE CAMBIOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
NO SE DISPONE DE UN PROCEDIMIENTO RESPECTO A LA GESTIÓN DE CAMBIOS DENTRO DE LA ENTIDAD	SE RECOMIENDA DISEÑAR E IMPLEMENTAR UN PROCEDIMIENTO PARA LA GESTIÓN DE CAMBIOS DENTRO DE LA ENTIDAD QUE AFECTEN A PROCESOS CLAVE, SISTEMAS O INSTALACIONES	

SEGURIDAD DE LOS RECURSOS, DESPACHOS Y OFICINAS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
NO SE DISPONE DE UNA POLÍTICA RESPECTO A LA SEGURIDAD DE LOS RECURSOS, DESPACHOS Y OFICINAS	SE RECOMIENDA DISEÑAR E IMPLEMENTAR UNA POLÍTICA DE SEGURIDAD DE LOS RECURSOS, DESPACHOS Y OFICINAS PARA EVITAR RIESGOS ANTE ACCESOS NO AUTORIZADOS, DAÑOS O PÉRDIDAS	

CONTROL DE ACCESO FÍSICO		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
LA POLÍTICA PARA EL CONTROL DE ACCESO FÍSICO NO SE MANTIENE ACTUALIZADA	SE DEBERÁ MANTENER ACTUALIZADA LA POLÍTICA Y, ADEMÁS, COMUNICARLA A TODO EL PERSONAL IMPLICADO SIEMPRE QUE EXISTA ALGÚN CAMBIO	
NO SE HA IMPLEMENTADO LA POLÍTICA DE CONTROL DE ACCESO FÍSICO	SE DEBERÁ IMPLEMENTAR LA PRESENTE POLÍTICA PARA EVITAR RIESGOS DE ACCESOS NO AUTORIZADOS	
NO SE DISPONE DE ZONAS RESTRINGIDAS PARA EL ALMACENAMIENTO DE DATOS DE CATEGORÍA ESPECIAL	SE DEBERÁN CONSIDERAR MECANISMOS DE SEGURIDAD PARA EL ACCESO A ZONAS RESTRINGIDAS SOLAMENTE A PERSONAL AUTORIZADO	
NO DISPONE DE UNA RELACIÓN ACTUALIZADA DE LAS AUTORIZACIONES PARA EL ACCESO A LAS INSTALACIONES DE LA ENTIDAD	SE RECOMIENDA MANTENER ACTUALIZADA LA RELACIÓN DE LAS PERSONAS AUTORIZADAS A ACCEDER A LAS INSTALACIONES DONDE SE REALIZAN TRATAMIENTOS DE INFORMACIÓN	
NO SE REGISTRAN LOS ACCESOS A LOS SISTEMAS DE INFORMACIÓN	SE RECOMIENDA REGISTRAR TODOS LOS ACCESOS A LOS SISTEMAS DE INFORMACIÓN	

PROCEDIMIENTOS DE TRATAMIENTOS NO AUTOMATIZADOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO

NO SE DISPONE DE UN PROCEDIMIENTO DE ETIQUETADO Y MANIPULACIÓN DE LA INFORMACIÓN	SE RECOMIENDA DISEÑAR E IMPLEMENTAR UN PROCEDIMIENTO PARA EL ETIQUETADO DE LA INFORMACIÓN DONDE SE REFLEJE LOS ACTIVOS DE INFORMACIÓN RELACIONADOS	
NO SE DISPONE DE MECANISMOS DE SEGURIDAD FÍSICAS PARA LOS DISPOSITIVOS DE ALMACENAMIENTO	SE DEBERÁN CONSIDERAR MECANISMOS PARA EVITAR LOS ACCESOS NO AUTORIZADOS A LA INFORMACIÓN DE LOS DISPOSITIVOS DE ALMACENAMIENTO	
NO SE HAN ADOPTADO MEDIDAS ALTERNATIVAS QUE IMPIDAN EL ACCESO A PERSONAS NO AUTORIZADAS	CUANDO LOS DISPOSITIVOS DE ALMACENAMIENTO NO DISPONGAN DE MEDIDAS DE SEGURIDAD FÍSICAS, SE DEBERÁN ESTABLECER MEDIDAS ALTERNATIVAS PARA EVITAR ACCESOS NO AUTORIZADOS	
NO SE CUSTODIA CORRECTAMENTE LA DOCUMENTACIÓN CUANDO NO SE ENCUENTRA EN SU LUGAR HABITUAL	SE DEBERÁ CONSIDERAR LA ADOPCIÓN DE MEDIDAS PARA LA CUSTODIA CORRECTA DE LOS SOPORTES CUANDO NO SE ENCUENTREN EN SU LUGAR HABITUAL	
NO SE MANTIENE ACTUALIZADA LA POLÍTICA/PROCEDIMIENTO RESPECTO A LOS SOPORTES FÍSICOS EN TRÁNSITO	SE DEBERÁ MANTENER ACTUALIZADA LA POLÍTICA/PROCEDIMIENTO PARA EVITAR ACCESOS NO AUTORIZADOS, USOS INDEBIDOS O, SIMPLEMENTE, DETERIORO	
NO SE IMPLANTADO LA POLÍTICA/PROCEDIMIENTO RESPECTO A LOS SOPORTES FÍSICOS EN TRÁNSITO	SE DEBERÁ APLICAR DE FORMA ACTIVA LA PRESENTE POLÍTICA/PROCEDIMIENTO PARA QUE TODO EL PERSONAL AFECTADO ESTÉ CONCIENCIADO DE LAS MEDIDAS ADOPTADAS	

9.2. SEGURIDAD INFORMÁTICA

SEGURIDAD EN LOS EQUIPOS INFORMÁTICOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
NO EXISTEN PROCEDIMIENTOS RESPECTO A LAS OPERACIONES DE LOS ACTIVOS DE INFORMACIÓN	SE DEBERÁ DISEÑAR Y, ADEMÁS, PONER A DISPOSICIÓN DE LAS PERSONAS IMPLICADAS LOS PROCEDIMIENTOS DE OPERACIÓN COMO MANTENIMIENTO DE LOS EQUIPOS, COPIAS DE SEGURIDAD Y/O GESTIÓN DE SOPORTES	
NO EXISTEN PROCEDIMIENTOS RESPECTO AL MANTENIMIENTO DE LOS EQUIPOS	SE DEBERÁ DISEÑAR UN CONJUNTO DE PROCEDIMIENTOS RESPECTO AL MANTENIMIENTO DE LOS EQUIPOS INFORMÁTICOS PROPIEDAD DE LA ENTIDAD	
NO SE MANTIENE ACTUALIZADO EL PROCEDIMIENTO RESPECTO A LA SALIDA DE ACTIVOS FUERA DE LOS LOCALES DE LA ENTIDAD	SE DEBERÁ MANTENER ACTUALIZADO EL PROCEDIMIENTO RESPECTO A LA SALIDA DE ACTIVOS SIEMPRE QUE EXISTA ALGÚN CAMBIO SIGNIFICATIVO EN EL MISMO	
NO SE HA IMPLEMENTADO EL PROCEDIMIENTO RESPECTO A LA SALIDA DE ACTIVOS FUERA DE LOS LOCALES DE LA ENTIDAD	SE DEBERÁ APLICAR DE FORMA ACTIVA EL PROCEDIMIENTO PARA EVITAR RIESGOS DE INTEGRIDAD Y CONFIDENCIALIDAD	

LA RELACIÓN DE ACTIVOS AUTORIZADOS NO SE MANTIENE ACTUALIZADA	SE DEBERÁ MANTENER ACTUALIZADA LA RELACIÓN DE AUTORIZACIONES PARA SACAR FUERA DE LAS INSTALACIONES LOS ACTIVOS DE INFORMACIÓN	
NO SE MANTIENEN ACTUALIZADOS LOS PROCEDIMIENTOS RESPECTO A LA ELIMINACIÓN DE EQUIPOS	SE DEBERÁN MANTENER ACTUALIZADOS LOS PROCEDIMIENTOS RESPECTO A LA ELIMINACIÓN DE EQUIPOS SIEMPRE QUE EXISTA ALGÚN CAMBIO EN LOS MISMOS	
NO SE HAN IMPLEMENTADO LOS PROCEDIMIENTOS RESPECTO A LA ELIMINACIÓN DE EQUIPOS	SE DEBERÁ APLICAR DE FORMA ACTIVA LOS PRESENTES PROCEDIMIENTOS PARA EVITAR EL ACCESO A DATOS DE CARÁCTER PERSONAL A PERSONAS NO AUTORIZADAS E, INCLUSO, FUGAS DE INFORMACIÓN	
NO SE MANTIENEN ACTUALIZADOS LOS PROCEDIMIENTOS RESPECTO A LOS EQUIPOS DESATENDIDOS	SE DEBERÁN MANTENER ACTUALIZADOS LOS PROCEDIMIENTOS RESPECTO A LOS EQUIPOS DESATENDIDOS DE LA ENTIDAD SIEMPRE QUE EXISTA ALGÚN CAMBIO EN LOS MISMOS	
NO SE HAN IMPLEMENTADO LOS PROCEDIMIENTOS RESPECTO A LOS EQUIPOS DESATENDIDOS	SE DEBERÁ APLICAR DE FORMA ACTIVA LOS PROCEDIMIENTOS PARA EVITAR EL ACCESO A PERSONAS NO AUTORIZADAS QUE PUDIERAN CONLLEVAR RIESGOS QUE AFECTEN A LA CONFIDENCIALIDAD, INTEGRIDAD E INCLUSO DISPONIBILIDAD	
NO EXISTEN PROCEDIMIENTOS RESPECTO A LOS SISTEMAS OPERATIVOS Y APLICACIONES DE LA ENTIDAD	SE DEBERÁ DISEÑAR UN PROCEDIMIENTO RESPECTO A LA GESTIÓN DE APLICACIONES Y SISTEMAS OPERATIVOS DE LA ENTIDAD PARA EVITAR LA INSTALACIÓN Y USO DE PROGRAMAS NO ADMITIDOS POR LA ENTIDAD	
NO SE MANTIENE ACTUALIZADO EL PROCEDIMIENTO RESPECTO A LAS RESTRICCIONES DE APLICACIONES DE LA ENTIDAD	SE DEBERÁ MANTENER ACTUALIZADO EL PROCEDIMIENTO RESPECTO A LA APLICACIÓN DE RESTRICCIONES EN REFERENCIA AL SOFTWARE Y SISTEMAS OPERATIVOS DE LA ENTIDAD	
NO SE HA IMPLEMENTADO EL PROCEDIMIENTO RESPECTO A LAS RESTRICCIONES DE APLICACIONES DE LA ENTIDAD	SE DEBERÁ APLICAR DE FORMA ACTIVA EL PRESENTE PROCEDIMIENTO PARA HACER FRENTE LA INTRODUCCIÓN DE VULNERABILIDADES EN LOS SISTEMAS, PÉRDIDA DE INTEGRIDAD O BIEN OTROS INCIDENTES QUE AFECTEN A LA SEGURIDAD DE LA INFORMACIÓN	
LA POLÍTICA/PROCEDIMIENTO RESPECTO A LA GESTIÓN DE LAS REDES NO SE MANTIENE ACTUALIZADA	SE DEBERÁ MANTENER ACTUALIZADO LA POLÍTICA/PROCEDIMIENTO RESPECTO A LA GESTIÓN DE LA SEGURIDAD EN LAS REDES DE COMUNICACIÓN SIEMPRE QUE EXISTA ALGÚN CAMBIO EN LOS MISMOS	
NO SE HA IMPLEMENTADO LA POLÍTICA/PROCEDIMIENTO RESPECTO A LA GESTIÓN DE LA SEGURIDAD DE LAS REDES DE LA ENTIDAD	SE DEBERÁ APLICAR DE FORMA ACTIVA LA POLÍTICA/PROCEDIMIENTO PARA EVITAR ACCESOS NO AUTORIZADOS O RIESGOS DE FUGAS DE INFORMACIÓN	

NO SE MANTIENE ACTUALIZADA LA POLÍTICA/PROCEDIMIENTO RESPECTO A LA MENSAJERÍA ELECTRÓNICA	SE DEBERÁ MANTENER ACTUALIZADO LA POLÍTICA O PROCEDIMIENTO RESPECTO A LA SEGURIDAD DEL USO EN MENSAJERÍA ELECTRÓNICA SIEMPRE QUE EXISTA ALGÚN CAMBIO SIGNIFICATIVO	
NO SE HA IMPLEMENTADO LA POLÍTICA/PROCEDIMIENTO RESPECTO A LA MENSAJERÍA ELECTRÓNICA	SE DEBERÁ APLICAR DE FORMA ACTIVA LA PRESENTE POLÍTICA O PROCEDIMIENTO Y COMUNICARLO AL PERSONAL QUE UTILICE HERRAMIENTAS DE MENSAJERÍA INSTANTÁNEA	

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE UBICACIÓN DE LOS SISTEMAS DE INFORMACIÓN		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
NO SE MANTIENE ACTUALIZADA LA POLÍTICA/PROCEDIMIENTO RESPECTO AL RÉGIMEN DE TRABAJO FUERA DE LA ENTIDAD	SE DEBERÁ MANTENER ACTUALIZADA LA POLÍTICA O PROCEDIMIENTO CUANDO EXISTAN CAMBIOS SIGNIFICATIVOS	
NO SE HA IMPLEMENTADO LA POLÍTICA/PROCEDIMIENTO RESPECTO AL RÉGIMEN DE TRABAJO FUERA DE LA ENTIDAD	SE DEBERÁ IMPLEMENTAR LA POLÍTICA RESPECTO AL RÉGIMEN DE TRABAJO FUERA DE LA ENTIDAD PARA QUE LA INFORMACIÓN TRATADA NO SE VEA COMPROMETIDA	

GESTIÓN DE USUARIOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
LA POLÍTICA/PROCEDIMIENTO RESPECTO A LA GESTIÓN DE LOS USUARIOS NO SE MANTIENE ACTUALIZADA	SE DEBERÁ MANTENER ACTUALIZADA LA POLÍTICA O PROCEDIMIENTO CUANDO EXISTAN CAMBIOS SIGNIFICATIVOS	
NO SE HA IMPLEMENTADO DE FORMA ACTIVA LA POLÍTICA/PROCEDIMIENTO RESPECTO A LA GESTIÓN DE LOS USUARIOS	SE DEBERÁ IMPLEMENTAR LA POLÍTICA RESPECTO LA GESTIÓN DE USUARIOS PARA EVITAR RIESGOS DE ACCESOS NO AUTORIZADOS	

INVENTARIO DE APLICACIONES INFORMÁTICAS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
EL PROCEDIMIENTO RESPECTO AL INVENTARIO DE APLICACIONES INFORMÁTICAS NO SE MANTIENE ACTUALIZADO	SE DEBERÁ MANTENER ACTUALIZADA EL PROCEDIMIENTO CUANDO EXISTAN CAMBIOS SIGNIFICATIVOS	
NO SE DISPONE DE UNA RELACIÓN ACTUALIZADA DE LAS APLICACIONES	SE RECOMIENDA MANTENER ACTUALIZADA LA RELACIÓN DE LAS APLICACIONES PERMITIDAS DENTRO DE LA ENTIDAD	

NO SE HA IMPLEMENTADO EL PROCEDIMIENTO RESPECTO AL INVENTARIO DE APLICACIONES INFORMÁTICAS	SE DEBERÁ APLICAR DE FORMA ACTIVA Y, ADEMÁS, COMUNICAR A TODO EL PERSONAL INVOLUCRADO EL PROCEDIMIENTO RESPECTO AL INVENTARIO DE APLICACIONES	

GESTIÓN DE SOPORTES		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
EL PROCEDIMIENTO RESPECTO A LA GESTIÓN DE SOPORTES NO SE MANTIENE ACTUALIZADO	SE DEBERÁ MANTENER ACTUALIZADO EL PROCEDIMIENTO SIEMPRE QUE EXISTA ALGÚN CAMBIO SIGNIFICATIVO	
NO SE HA IMPLEMENTADO EL PROCEDIMIENTO RESPECTO A LA GESTIÓN DE SOPORTES	SE DEBERÁ IMPLEMENTAR EL PROCEDIMIENTO Y COMUNICARLO A TODO EL PERSONAL INVOLUCRADO	

PROCEDIMIENTO DE COPIAS DE SEGURIDAD Y RECUPERACIÓN		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
EL PROCEDIMIENTO PARA LA REALIZACIÓN DE COPIAS DE SEGURIDAD NO SE MANTIENE ACTUALIZADO	SE DEBERÁ MANTENER ACTUALIZADO EL PROCEDIMIENTO PARA LA REALIZACIÓN DE COPIAS DE SEGURIDAD SIEMPRE QUE EXISTA UN CAMBIO SIGNIFICATIVO	
NO SE HA IMPLEMENTADO EL PROCEDIMIENTO PARA LA REALIZACIÓN DE COPIAS DE SEGURIDAD	SE DEBERÁ APLICAR DE FORMA ACTIVA Y, ADEMÁS, COMUNICARLO A TODO EL PERSONAL INVOLUCRADO EL PROCEDIMIENTO PARA LA REALIZACIÓN DE COPIAS DE SEGURIDAD	

POLÍTICA DE CONTROLES CRIPTOGRÁFICOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
LA POLÍTICA DE CONTROLES CRIPTOGRÁFICOS NO SE MANTIENE ACTUALIZADA	LA POLÍTICA DE CONTROLES CRIPTOGRÁFICOS SE DEBERÁ MANTENER ACTUALIZADA SIEMPRE QUE EXISTA ALGÚN CAMBIO SUSTANCIAL EN LA MISMA	
NO SE HA IMPLEMENTADO LA POLÍTICA DE CONTROLES CRIPTOGRÁFICOS	LA POLÍTICA DE CONTROLES CRIPTOGRÁFICOS SE DEBERÁ IMPLEMENTAR Y COMUNICAR A TODO EL PERSONAL IMPLICADO	

9.3. SEGURIDAD EN LA RELACIÓN CON TERCEROS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
LA POLÍTICA/PROCEDIMIENTO EN RELACIÓN CON TERCERAS PARTES NO SE MANTIENE ACTUALIZADA	SE DEBERÁ MANTENER ACTUALIZADA LA POLÍTICA/PROCEDIMIENTO EN RELACIÓN CON TERCERAS PARTES	

NO SE HA IMPLEMENTADO LA POLÍTICA/PROCEDIMIENTO EN RELACIÓN CON TERCERAS PARTES	SE DEBERÁ APLICAR DE FORMA ACTIVA Y, A SU VEZ, COMUNICARLA A TODO EL PERSONAL INVOLUCRADO LA POLÍTICA EN RELACIÓN CON TERCERAS PARTES	

9.4. GESTIÓN DE INCIDENCIAS Y VIOLACIONES DE SEGURIDAD DE LOS DATOS		
NO CONFORMIDAD	MEDIDA CORRECTORA	GRADO
NO SE ACTUALIZA EL PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES Y VIOLACIONES DE SEGURIDAD DE LOS DATOS	DISEÑAR Y APLICAR UN PROCEDIMIENTO ADECUADO PARA LA GESTIÓN DE LAS VIOLACIONES DE SEGURIDAD	
NO SE APLICA EL PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES Y VIOLACIONES DE SEGURIDAD DE LOS DATOS	ACTUALIZAR Y/O APLICAR EL PROCEDIMIENTO PARA LA GESTIÓN DE LAS VIOLACIONES DE SEGURIDAD	

11. DICTAMEN FINAL DEL INFORME DE AUDITORÍA

En BARCELONA a 7 de marzo de 2022,

Para finalizar el presente informe de auditoría independiente del cumplimiento de medidas de seguridad de las instalaciones y tratamientos de datos de carácter personal de personas físicas, a continuación se presenta la conclusión del mismo, con el objetivo de facilitar una adecuada visibilidad del grado de adecuación en que se encuentra EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL.

El presente dictamen, así como todo el análisis llevado a cabo a lo largo del presente informe, se emite de acuerdo con la situación vigente en el momento de la toma de datos, realizada el pasado día 17 de enero de 2022.

Una vez llevado a cabo el correspondiente análisis de cumplimiento, que se desprende del presente informe, en opinión del auditor y, analizadas sus políticas, protocolos y procedimientos, estos son adecuados a lo establecido por la normativa vigente en protección de datos, exceptuando las NO CONFORMIDADES analizadas a lo largo del presente informe de auditoría, relacionadas en el apartado 10, y que deberán ser subsanadas por parte de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL.

Se pone en conocimiento de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL que se encuentra sujeta al régimen sancionador establecido en la normativa vigente en materia de Protección de Datos, dependiendo del artículo que haya sido vulnerado, y sin perjuicio del derecho de indemnización que el Interesado podrá reclamar judicialmente, las sanciones impuestas sobre infracciones al Reglamento General de Protección de Datos pueden ascender a los 10 millones de euros (o el 2% como máximo del volumen de negocio total anual global) hasta los 20 millones de euros (o el 4% como máximo del volumen de negocio total anual global), que en lo que infiere al ámbito nacional se encuentra regulado por los artículos 70 a 78 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En último lugar, el Responsable de seguridad/privacidad de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL debe analizar el presente informe de auditoría y elevar a la dirección de EPISTEME INVESTIGACION E INTERVENCIÓN SOCIAL las presentes conclusiones, que resulten para que esta adopte las medidas correctoras adecuadas y, por otro lado, que el presente documento deberá estar a disposición de la autoridad de control competente, con el objeto de evidenciar el cumplimiento del principio de proactividad.

Firmado:

Departamento Auditoría

PROFESSIONAL GROUP CONVERSIA SLU

CONVERSIA